PRONOVA
SOLUÇÕES
INTELIGENTES

BioPass3000

Manual do Usuário
Versão 2.0

Pronova Soluções Inteligentes
http://www.pronova.com.br

As informações contidas neste manual estão sujeitas a alterações sem aviso prévio e não representam um compromisso por parte de PRONOVA CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO LTDA. Nenhuma parte deste manual poderá ser reproduzida de qualquer forma ou meio, eletrônico ou mecânico, incluindo fotocópia, gravação ou sistemas de armazenamento e recuperação, sem o prévio consentimento, por escrito, de PRONOVA CONSULTORIA EM TECNOLOGIA DA INFORMAÇÃO LTDA.

Windows® é marca registrada da Microsoft Corporation
Pentium® é marca registrada da Intel Corporation
EnterSafe é marca registrada da Feitian Technologies Inc., Ltd.
ePassNG é marca registrada da Feitian Technologies Inc., Ltd.
ROCKEY é marca registrada da Feitian Technologies Inc., Ltd.
AMD® é marca registrada Advanced Micro Devices

Pronova Consultoria em Tecnologia da Informação Ltda.

& Feitian Technologies Co., Ltd.

Todos os produtos da FEITIAN Technologies Co., Ltd. (FEITIAN) e da Pronova Soluções Inteligentes (PRONOVA) incluindo, sem limitar-se a, cópias de avaliação, disquetes, CD-ROMs, hardware, software e documentação, e todos os futuros pedidos, estão sujeitos aos termos deste Contrato. Se você não está de acordo com os termos aqui expostos, por favor, proceda a devolução do pacote completo e dentro do prazo de quinze dias úteis e reembolsaremos o custo do produto, exceto o frete e os encargos administrativos. Ao utilizar o produto você declara conhecer e aceitar os termos e condições do presente, que se formalizará em um contrato de Licença entre você e a FEITIAN, que também terá alcance aos distribuidores, revendas ou representantes da FEITIAN, com o alcance aqui convencionado.

1. **Uso Permitido** – Você pode fundir, relacionar e/ou fazer link do Software com outros programas com o único propósito de proteger esses programas de acordo com o uso descrito no Guia do Desenvolvedor que está junto com o produto, ou que pode ser encontrado no site web da FEITIAN (www.ftsafe.com) ou da PRONOVA (www.pronova.com.br). Você pode realizar cópias do Software com o fim de utilizá-las como cópias de segurança ou backup.

2. **Uso proibido** – -O Software ou o hardware fornecido pela FEITIAN/PRONOVA ou qualquer outra parte do Produto não pode ser reproduzida, copiada, reinventada, desasemblada, descompilada, revisada, melhorada e modificada de qualquer forma, exceto como especificamente se permite no presente. Você não pode praticar engenharia reversa ao Software ou qualquer parte do produto, ou tentar descobrir o código fonte do Software. Você não pode usar o meio ótico ou magnético incluído com o produto com o propósito de transferir ou guardar dados que não fazem parte original de Produto, ou uma melhora ou atualização de Produto fornecida pela FEITIAN ou pela PRONOVA.

POLÍTICA DE GARANTIA PRONOVA

IMPORTANTE-LEIA ESTA GARANTIA DO FABRICANTE COM ATENÇÃO PARA ENTENDER SEUS DIREITOS E OBRIGAÇÕES! O termo "Dispositivo de Hardware" significa o produto de hardware Pronova. O termo "Você" significa uma pessoa física ou jurídica que será referida nesta Garantia Limitada como *"Você"* e "Seu(s)/Sua(s)".

A. GARANTIAS.

1. Garantia Expressa. *Você* estará sujeito aos termos e condições desta Garantia Limitada e, em substituição a quaisquer outras (se houver) garantias expressas, a Pronova garante a *Você,* sob condições normais de uso e serviço, na data da aquisição identificada no recibo ou no comprovante de pagamento e pelo período de tempo especificado abaixo para o Dispositivo de Hardware aplicável (doravante denominados o "Prazo de Garantia"), que o Dispositivo de Hardware será executado substancialmente em conformidade com o descrito na embalagem e na documentação da Pronova que o acompanha.

A PRONOVA assegura total cobertura contra defeito de fabricação para os produtos fornecidos ao cliente no território brasileiro, durante o período da garantia.

Prazo de Garantia

Garantia Legal - 90 (noventa) dias

A garantia legal praticada pela PRONOVA obedece aos dispositivos relacionados no artigo 26 do Código de Defesa do Consumidor (CDC), e é direito do consumidor que apresente a reclamação comprovadamente formulada no prazo de 90 (noventa) dias da data de aquisição do produto PRONOVA para troca do produto e/ou serviço adquirido por igual ou equivalente superior.

A reposição dos produtos em garantia estará sujeita às condições de retorno do produto, observando a garantia legal, conforme art. 50 do CDC.

PRAZO TOTAL DA GARANTIA:

(I) Para todos os conjuntos de Tokens USB: 90 (noventa) dias;

(II) Leitor de cartão inteligente: 90 (noventa) dias;

(III) Cartão Inteligente: 90 (noventa) dias.

(IV) Dongles para proteção de software: 90 (noventa) dias.

Os dispositivos criptográficos (tokens e cartões) e leitores de cartão inteligente vendidos pela PRONOVA tem garantia contra defeitos de fabricação pelo prazo de 90 (noventa) dias contados a partir da data de aquisição do produto PRONOVA.

Os dispositivos criptográficos (tokens e cartões) armazenam o seu Certificado Digital protegendo-o contra acessos indevidos. AS SENHAS (PIN, PUK, SENHA, FRASE SENHA OU PASSWORD) PARA ACESSO A ESSES DISPOSITIVOS SÃO SOMENTE DE CONHECIMENTO E RESPONSABILIDADE DO TITULAR OU RESPONSÁVEL DO CERTIFICADO DIGITAL, E A PRONOVA NÃO MANTÉM CÓPIAS OU POSSUI MEIOS DE RECUPERÁ-LAS.

CASO O DISPOSITIVO CRIPTOGRÁFICO SEJA BLOQUEADO OU INUTILIZADO DEVIDO À PERDA DAS SENHAS, SEU CONTEÚDO SERÁ PERDIDO. A REPOSIÇÃO DESTES DISPOSITIVOS (E DE SEU CONTEÚDO) NÃO É COBERTA PELA POLÍTICA DE GARANTIA PRONOVA.

Caso o Serviço de Suporte Técnico PRONOVA constate defeito de fabricação que requeira a substituição do dispositivo criptográfico durante o período de vigência desta garantia, a PRONOVA:

- Efetuará troca do dispositivo criptográfico, sem custo adicional para o cliente; e

- Não emitirá um novo certificado, sem custo adicional para o cliente, caso o defeito de fabricação acarrete na perda do Certificado Digital.

Essa Garantia Limitada não cobrirá, bem como não será fornecido qualquer tipo de garantia para aspectos subjetivos ou estéticos do Dispositivo de Hardware. A garantia expressa prevista acima constitui a única garantia expressa concedida a Você e é fornecida em substituição a todas as outras condições e garantias, sejam expressas ou implícitas (exceto quaisquer garantias implícitas existentes que não possam ser recusadas), inclusive aquelas criadas por qualquer outra documentação ou embalagem. Qualquer informação ou sugestão (oral ou escrita) fornecida pela Pronova, por seus agentes, afiliadas ou subsidiárias ou por seus funcionários ou agentes, não criará qualquer garantia ou condição ou ampliará o escopo desta Garantia Limitada.

2. Limitação da Vigência das Garantias Implícitas. Se Você for um consumidor estrangeiro, também poderá ter uma condição e/ou garantia implícita de acordo com a legislação de algumas jurisdições, a qual é limitada pela vigência do presente Prazo de Garantia.

B. RECURSO EXCLUSIVO. Sujeito à legislação aplicável e às disposições a seguir, e desde que Você, durante o Prazo de Garantia, devolva o Dispositivo de Hardware à Pronova, com uma cópia do recibo ou comprovante válido de pagamento, a Pronova irá, a seu critério:

(i) reparar ou substituir o Dispositivo de Hardware; ou (ii) indenizá-lo pelos danos diretos sofridos por Você, limitando-se a responsabilidade ao valor efetivamente pago por Você pelo Dispositivo de Hardware.

(ii) Qualquer Dispositivo de Hardware reparado ou substituído conforme esta Garantia Limitada terá garantia pelo Prazo de Garantia original remanescente ou por 30 (trinta) dias, a partir da data de devolução do item para Você, o que for maior.

Salvo previsão expressa em contrário pela legislação aplicável, Você deverá arcar com os custos relacionados ao transporte (inclusive embalagem) do produto dentro do prazo da garantia; e

C. ISENÇÃO DE OUTRAS GARANTIAS. A garantia expressa especificada acima é a única garantia expressa oferecida a Você e é fornecida em substituição a todas as outras condições e garantias expressas ou implícitas (se houver), inclusive aquelas criadas por qualquer outra documentação ou embalagem. Nenhuma outra garantia é fornecida em relação ao Dispositivo de Hardware ou aos serviços de garantia por qualquer pessoa, incluindo, mas não se limitando a, a Pronova, os seus agentes, as afiliadas e os fornecedores. Nenhuma informação ou sugestão (oral ou escrita) fornecida pela Pronova, por seus agentes, afiliadas ou subsidiárias ou por seus funcionários ou agentes, deverá criar uma garantia ou condição ou ampliar o escopo desta Garantia Limitada. Também não há garantias ou condições de titularidade, uso pacífico ou não-violação de direitos de autor no Dispositivo de Hardware.

D. EXCLUSÃO DE OUTROS DANOS.

NA EXTENSÃO MÃXIMA PERMITIDA PELA LEGISLAÇÃO APLICÁVEL, A PRONOVA, SEUS AGENTES, AFILIADAS E/OU FORNECEDORES NÃO SERÃO RESPONSÁVEIS POR QUALQUER:

(i) DANO CONSEQÜENCIAL OU INCIDENTAL;

(ii) DANOS POR LUCROS CESSANTES, INTERRUPÇÃO DE NEGÓCIOS, PERDA DE DADOS, INFORMAÇÕES CONFIDENCIAIS OU OUTRAS, PERDA DE PRIVACIDADE, QUALQUER INABILIDADE NO USO DO DISPOSITIVO DE HARDWARE, NO TODO OU EM

PARTE, DANOS PESSOAIS OU QUALQUER FALHA NO CUMPRIMENTO DE QUALQUER OBRIGAÇÃO (INCLUINDO MAS NÃO SE LIMITANDO A QUALQUER OBRIGAÇÃO GERADA EM RELAÇÃO A CASO DE NEGLIGÊNCIA E QUEBRA DO PRINCÍPIOS DE BOA-FÉ E DO ESFORÇO DE APRIMORAMENTO);

(iii) DANO INDIRETO, ESPECIAL OU PUNITIVO DECORRENTE DO OU DE QUALQUER FORMA RELACIONADO COM O DISPOSITIVO DE HARDWARE.

(iii) QUALQUER TIPO DE INFORMAÇÃO QUE VENHA A SER ARMAZENADA NOS EQUIPAMENTOS COMERCIALIZADOS PELA PRONOVA.

AS EXCLUSÕES ACIMA SERÃO APLICADAS MESMO QUE A PRONOVA OU QUALQUER AGENTE, AFILIADA OU FORNECEDOR TENHA SIDO ALERTADO SOBRE A POSSIBILIDADE DE OCORRÊNCIA DE TAIS PERDAS OU DANOS, E MESMO QUE HAJA FALHA, DANO (INCLUSIVE NEGLIGÊNCIA), RESPONSABILIDADE OBJETIVA OU PELO FATO DO PRODUTO, DECLARAÇÃO FALSA OU QUALQUER OUTRO MOTIVO.

E. EXCLUSÕES DE COBERTURA. A Garantia Limitada não será aplicável e a Pronova, seus agentes, afiliadas e/ou fornecedores não terão qualquer responsabilidade relativa a esta Garantia Limitada se o Dispositivo de Hardware:

(i) for usado para fins comerciais (inclusive aluguel ou arrendamento);

(ii) for modificado ou adulterado;

(iii) for danificado por motivos de força maior, alta-tensão, uso indevido, abuso, negligência, acidente, desgaste, manipulação indevida, aplicação errada ou outras causas não relacionadas a defeitos no Dispositivo de Hardware;

(iv) for danificado por programas, informações, vírus ou arquivos ou durante envios ou transmissões;

(v) não for usado de acordo com a documentação e as instruções de uso que o acompanham; ou

(vi) for reparado, modificado ou alterado por outra pessoa que não seja um representante da assistência técnica autorizada da Pronova e se a assistência técnica não autorizada causar ou contribuir para o surgimento de qualquer defeito ou dano.

F. REGISTRO. Não é necessário registrar a aquisição do Dispositivo de Hardware para que essa Garantia Limitada tenha validade.

G. BENEFICIÁRIO. Na extensão máxima permitida pela lei aplicável, a Garantia Limitada será concedida exclusivamente a Você, o primeiro adquirente do Dispositivo de Hardware, não existindo outros beneficiários da Garantia Limitada. Salvo previsão expressa em contrário na lei, esta Garantia limitada não será destinada, bem como não será aplicável a qualquer outra pessoa, inclusive qualquer pessoa para a qual Você faça uma transferência do Dispositivo de Hardware.

H. INFORMAÇÕES ADICIONAIS. A Pronova é a entidade que fornece esta Garantia Limitada. Para receber instruções sobre como executar esta Garantia Limitada, entre em contato com uma subsidiária Pronova de sua localidade ou escreva para; Pronova Soluções Inteligente, Avenida das Américas 500, bloco 4, sala 302, Barra da Tijuca, Rio de Janeiro, RJ, CEP 22.640-100, ou visite a Pronova na Internet no endereço http//www.pronova.com.br

Outras exigências:

1. Você deverá enviar um comprovante de pagamento na forma de uma fatura (ou uma cópia) ou um recibo autêntico com data evidenciando que Você é o beneficiário desta Garantia Limitada e que a Sua solicitação está sendo feita dentro do Prazo de Garantia.

2. Para execução da Garantia Limitada, Você deverá levar ou enviar o item na sua embalagem

original ao local especificado pela Pronova. Salvo previsão expressa em contrário prevista na legislação aplicável, Você arcará com os custos relacionados ao transporte (inclusive embalagem) do serviço dentro do prazo da garantia.

Caso não siga as instruções acima, Você poderá ter despesas adicionais, poderá perder a sua garantia ou poderão ocorrer atrasos.

As informações contidas neste documento, incluindo URLs e outras referências a sites na Internet, estão sujeitas a alterações sem aviso prévio. Salvo indicação em contrário, os exemplos de empresas, organizações, produtos, nomes de domínio, endereços de email, logotipos, pessoas, lugares e acontecimentos aqui mencionados são fictícios e nenhuma associação com qualquer empresa, organização, produto, nome de domínio, endereço de e-mail, logotipo, pessoa ou acontecimento real é intencional ou deve ser inferida.

Obedecer a todas as leis de direitos autorais aplicáveis é responsabilidade do usuário. Sem limitar os direitos autorais, nenhuma parte deste documento pode ser reproduzida, armazenada ou introduzida em um sistema de recuperação, ou transmitida de qualquer forma por qualquer meio (eletrônico, mecânico, fotocópia, gravação ou qualquer outro), ou para qualquer propósito, sem a permissão expressa e por escrito da Pronova.

A Pronova pode ter patentes ou requisições para obtenção de patente, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual que abrangem o conteúdo deste documento. A posse deste documento não lhe confere nenhum direito sobre as citadas patentes, marcas comerciais, direitos autorais ou outros direitos de propriedade intelectual, salvo aqueles expressamente mencionados em um contrato de licença, por escrito, da Pronova.

© 2004 Pronova Soluções Inteligentes. Todos os direitos reservados.

ePass, ePassNG, EnterSafe, ePass1000, ePass2000, ePass3000, Rockey e BioPass3000 são marcas registradas ou comerciais da Feitian Technologies Co., Inc. na República Popular da China e/ou em outros países.

Pronova e ProToken são marcas registradas ou comerciais da Pronova Consultoria em Tecnologia da Informação Ltda. na República Federativa do Brasil e/ou em outros países.

Os nomes de produtos e de empresas reais aqui mencionados podem ser marcas comerciais de seus respectivos proprietários.

A Pronova concede ao comprador deste produto o direito de reproduzir uma (1) cópia do "Manual de Instruções" impresso para cada Dispositivo de Hardware adquirido na embalagem.

Atestado de Conformidade EC

CE

O equipamento obedece ao principal requerimento de proteção da Diretiva EMC (Diretiva 89/336/EEC relativa à compatibilidade eletromagnética) baseada em um teste voluntário.

Este certificado se refere somente a um exemplo particular do produto e a documentação técnica deste fornecida para teste e certificação. Os resultados detalhados e todos os padrões usados, bem como o modo de operação estão listados em:

Relatório Teste No.: 70407310011

Testes Realizados: EN 55022/1998 EN 55024/1998

Após a preparação da documentação técnica necessária, bem como a declaração de conformidade CE a marca exibida acima pode ser fixado no equipamento como estipulado no Artigo 10.1 da Diretiva. Outras diretivas relevantes devem ser observadas.

Certificado de Aprovação FCC

Este dispositivo está em conformidade com a Parte 15 das Regras FCC e Regulamentações para Equipamentos de Tecnologia da Informação.

USB

Este equipamento está baseado nos padrões USB.

WEEE (Waste Electrical and Electronic - Descarte de Equipamentos Elétricos e Eletrônicos)

A Diretiva Européia 2002/96/CE exige que o equipamento que exibe este símbolo no produto e/ou na sua embalagem não seja eliminado junto com os resíduos municipais não separados. O símbolo indica que este produto deve ser eliminado separadamente dos resíduos domésticos regulares. É sua responsabilidade eliminar este e qualquer outro equipamento elétrico e eletrônico através dos postos de recolhimento designados pelas autoridades governamentais ou locais. A eliminação e reciclagem correta ajudarão a prevenir as conseqüências negativas para o ambiente e para a saúde humana. Para obter informações mais detalhadas sobre a forma de eliminar o sei equipamento antigo, entre em contato com as autoridades locais, serviços de eliminação de resíduos ou o estabelecimento comercial onde adquiriu o produto.

ÍNDICE

Introdução – Conhecendo o BioPass3000 6

Capítulo 1 – Software

1.1 Instalação do Software do BioPass3000 8

1.2 Removendo o Software do BioPass3000 10

Capítulo 2 – Ferramentas do BioPass3000

2.1 Entersafe PKI Manager 13

2.1.1 Interface 13

2.1.2 Operações 20

2.2 Fingerprint Manager 31

2.2.1 Interface 31

2.2.2 Operções 32

2.3 Fingerprint Tour 43

2.3.1 Interface 43

2.3.2 Introdução à captura de digitais 44

Capítulo 3 – Sobre o BioPass3000

3.1 Como conectar o BioPass3000 49

3.2 Como manusear o BioPass3000 50

3.3 Como passar o dedo no sensor 50

3.4 Exemplos 51

3.4.1 Como usar o Fingerprint Tour para coletar uma amostra 51

3.4.2 Como usar o Fingerprint Manager para cadastrar uma digital 52

3.4.3 Como usar o EnterSafe PKI Manager para fazer login 52

Apêndice 1 – Especificações Técnicas 53

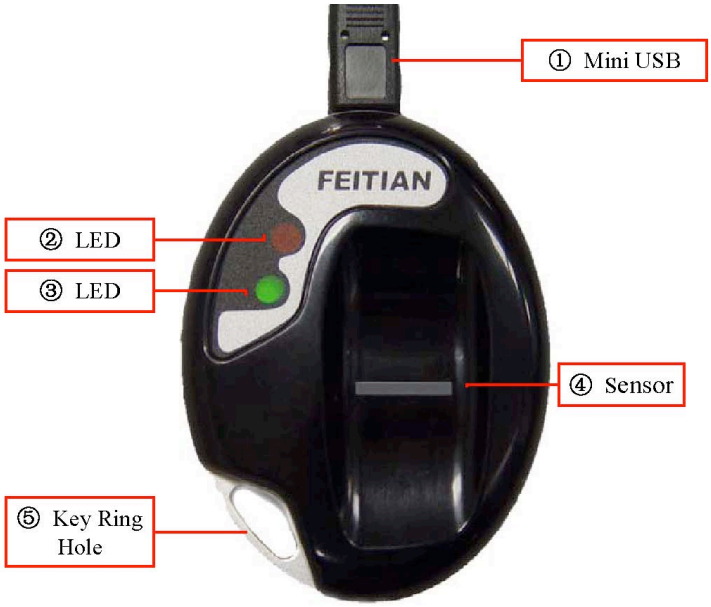
Apêndice 2 – Glossário de Termos 55

Garantia Limitada 56

Suporte

Contatos

INTRODUCÃO - Conhecendo o BioPass3000



1 - Mini USB

O token BioPass3000 se conecta ao computador através de um mini cabo USB. Por ser um dispositivo de baixo consumo de energia não necessita de uma fonte alimentação adicional. Para mais detalhes, leia a seção ***3.1 Como conectar***.

2 e 3 - LED

Existem dois LEDs no lado esquerdo do BioPass3000 que indicam o estado de funcionamento do dispositivo.

LED	ESTADO	DESCRIÇÃO
LED da digital **Vermelho**	Pisca rapidamente (a cada 2s)	Nenhuma digital cadastrada
	Apagada	Pronto
	Acesa	Esperando uma digital ou digital está sendo cadastrada
	Pisca rapidamente 2 vezes – pisca devagar 1 vez – apaga	Falha de hardware
LED de estado do token **Verde**	Acesa	Pronto
	Piscando (a cada 1s)	Driver não está instalado
	Piscando rapidamente de maneira irregular	Token ocupado (lendo ou escrevendo)

	Pisca rapidamente 2 vezes – pisca devagar 1 vez – apaga	Falha de hardware

4 – Sensor de digitais

5 - Entrada para chaveiro: O BioPass3000 possui uma entrada para chaveiro localizada na parte inferior esquerda do token. Assim, o usuário poderá ter o seu BioPass3000 sempre à mão de maneira prática.

CAPÍTULO 1 - Software

1.1 Instalação

Insira o CD de instalação e execute o arquivo **BioPass3000-English.exe** para iniciar o processo. Quando o *Setup Wizard* do BioPass3000 iniciar, uma janela como a da Figura 1-1 será exibida.

BioPass3000 Setup
Welcome to the BioPass3000 Setup Wizard
This wizard will guide you through the installation of BioPass3000.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Install to start the installation.
Install
Cancel

Figura 1-1: janela do Assistente de Instalação

Clique no botão **Install** para instalar o software.

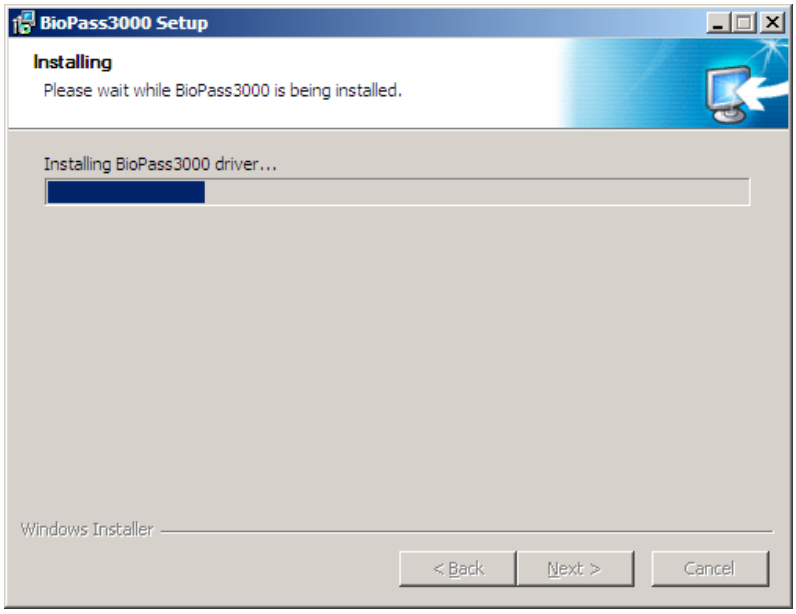


Figura 1-2: Instalando o software do BioPass3000

Nota: Se o usuário deseja aplicar as funções de certificação nos navegadores Netscape, Mozilla ou Firefox, o arquivo ESP11v211.dll precisa ser manualmente carregado.

Após finalizar a instalação, a seguinte janela será exibida, conforme a Figura 1-3.

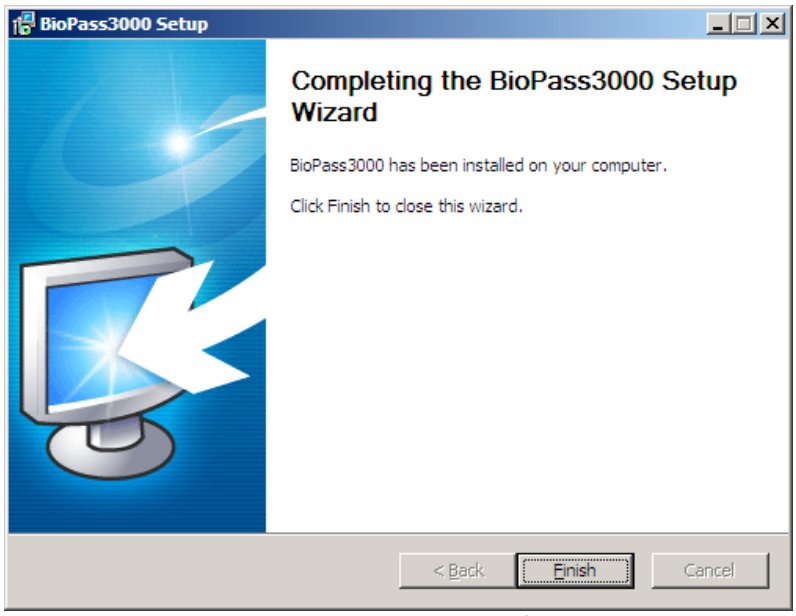


Figura 1-3: Finalizando a instalação do software do BioPass3000

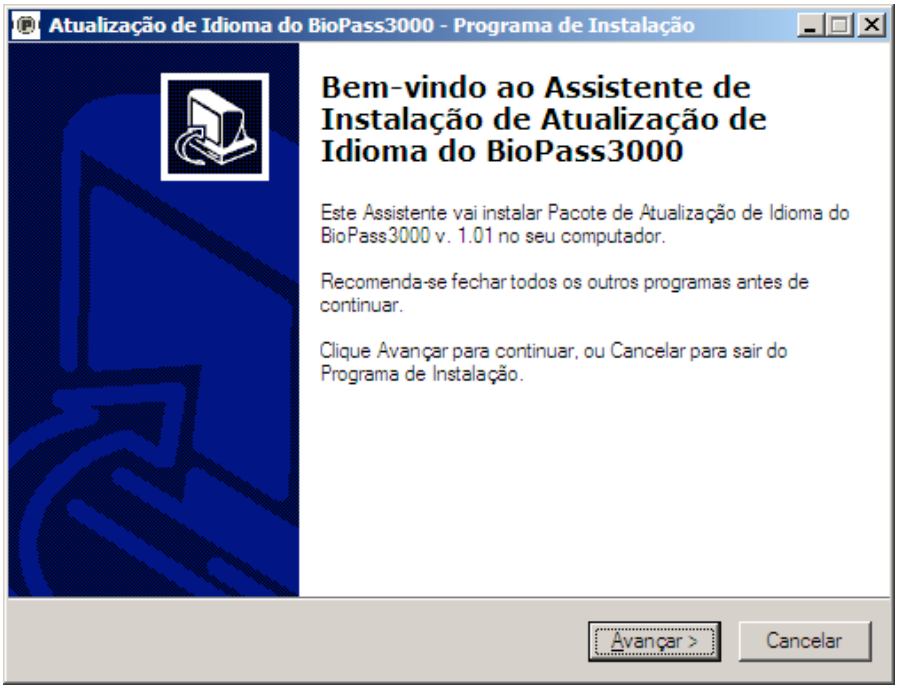
Clique no botão “Finish” para concluir a execução do Assistente de Instalação do BioPass3000.

Atualizando o software do BioPass3000 para o Idioma Português do Brasil

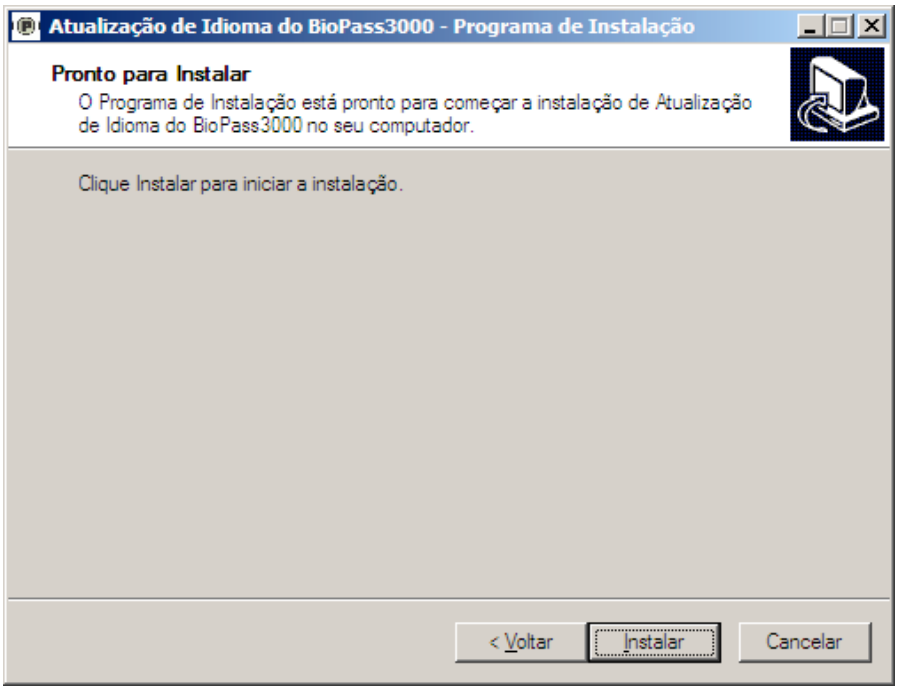
Para atualizar o software do BioPass3000 para Português do Brasil, execute o arquivo

Update.exe que está na raiz do CD-ROM de instalação do seu BioPass3000.

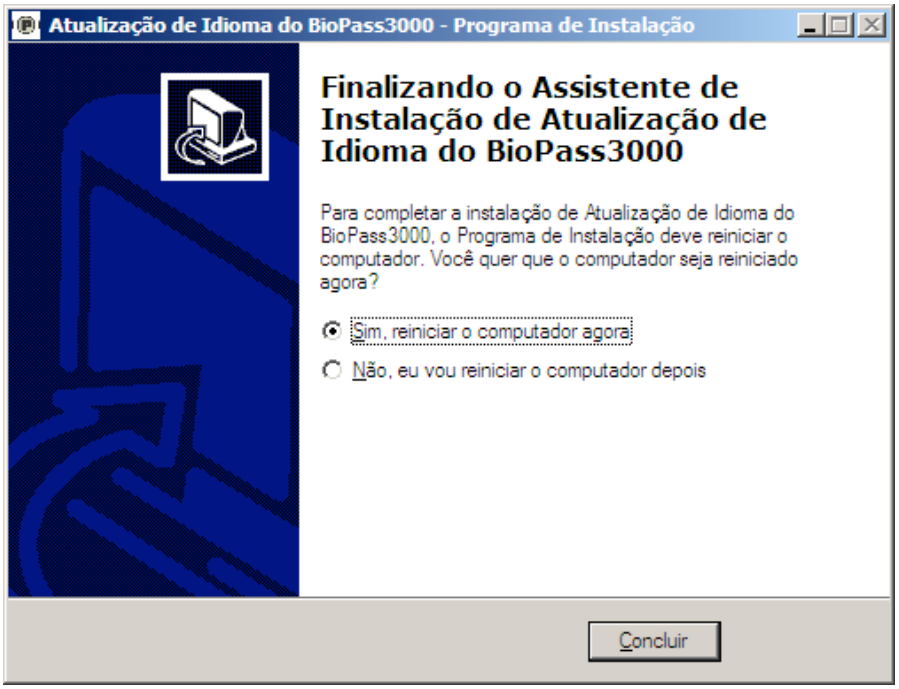
Clique em Avançar da janela de boas vindas


Atualização de Idioma do BioPass3000 - Programa de Instalação
Bem-vindo ao Assistente de Instalação de Atualização de Idioma do BioPass3000
Este Assistente vai instalar Pacote de Atualização de Idioma do BioPass3000 v. 1.01 no seu computador.
Recomenda-se fechar todos os outros programas antes de continuar.
Clique Avançar para continuar, ou Cancelar para sair do Programa de Instalação.
Avançar >
Cancelar

Clique no botão Instalar da próxima tela


Atualização de Idioma do BioPass3000 - Programa de Instalação
Pronto para Instalar
O Programa de Instalação está pronto para começar a instalação de Atualização de Idioma do BioPass3000 no seu computador.
Clique Instalar para iniciar a instalação.
< Voltar
Instalar
Cancelar

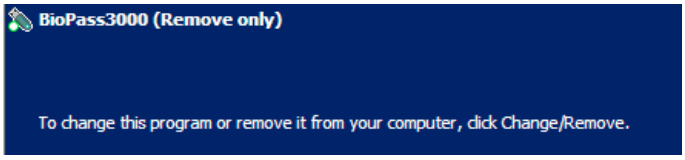
Aguarde a atualização e ao final, selecione a opção “Sim, reiniciar o computador agora” e clique no botão “Concluir”.


Atualização de Idioma do BioPass3000 - Programa de Instalação
Finalizando o Assistente de Instalação de Atualização de Idioma do BioPass3000
Para completar a instalação de Atualização de Idioma do BioPass3000, o Programa de Instalação deve reiniciar o computador. Você quer que o computador seja reiniciado agora?
Sim, reiniciar o computador agora
Não, eu vou reiniciar o computador depois
Concluir

1.2 Removendo o software do BioPass3000

Para remover o software do BioPass3000 você pode utilizar o recurso **Adicionar ou Remover Programas** do Windows, localizado no Painel de Controle.

Em **Adicionar ou Remover Programas**, procure na lista e selecione o item **"BioPass3000 (Remove Only)"**.



Clique no botão **Alterar/Remover** para iniciar o guia de remoção, como mostrado na Figura 1-5 abaixo.

BioPass3000 Uninstall
Welcome to the BioPass3000 Uninstall Wizard
This wizard will guide you through the uninstallation of BioPass3000.
Before starting the uninstallation, make sure BioPass3000 is not running.
Click Uninstall to start the uninstallation.
Uninstall
Cancel

Figura 1-5: Assistente para remover o software do BioPass3000

Clique no botão **Uninstall** (**Desinstalar)** para iniciar o processo automático de remoção. Veja a Figura 1-6 abaixo.

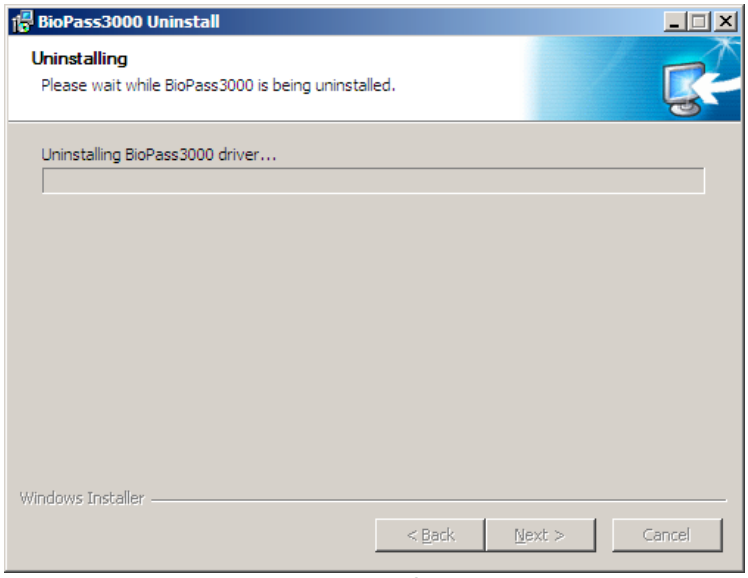


Figura 1-6: Removendo o software do BioPass3000

Ao final do processo, uma janela como a da Figura 1-7 será mostrada.

BioPass3000 Uninstall
Completing the BioPass3000 Uninstall Wizard
Your computer must be restarted in order to complete the uninstallation of BioPass3000. Do you want to reboot now?
Reboot now
I want to manually reboot later
< Back
Finish
Cancel

Figura 1-7: Fim da remoção do software do BioPass3000

Clique em **Finish** para reiniciar o computador e fechar o assistente de remoção do software do BioPass3000.

CAPÍTULO 2 – Ferramentas do BioPass3000

2.1 EnterSafe PKI Manager

Esta seção mostrará as principais funções do EnterSafe PKI Manager no sistema operacional Windows:

- Login (verificação da digital do usuário)
- Verificar do conteúdo do token
- Alterar o nome do token
- Gerenciar dados do token

Para abrir esta ferramenta, vá até **Iniciar | Programas | Feitian | BioPass3000** e clique em **EnterSafe PKI Manager**.

Nota: A indicação "Administrator Version" se refere à versão atual do EnterSafe PKI Manager do BioPass3000.

2.1.1 Interface

- *Interface com token desconectado:* inicie o Gerenciador PKI EnterSafe. Uma janela como a da Figura 2-1-1 será exibida:

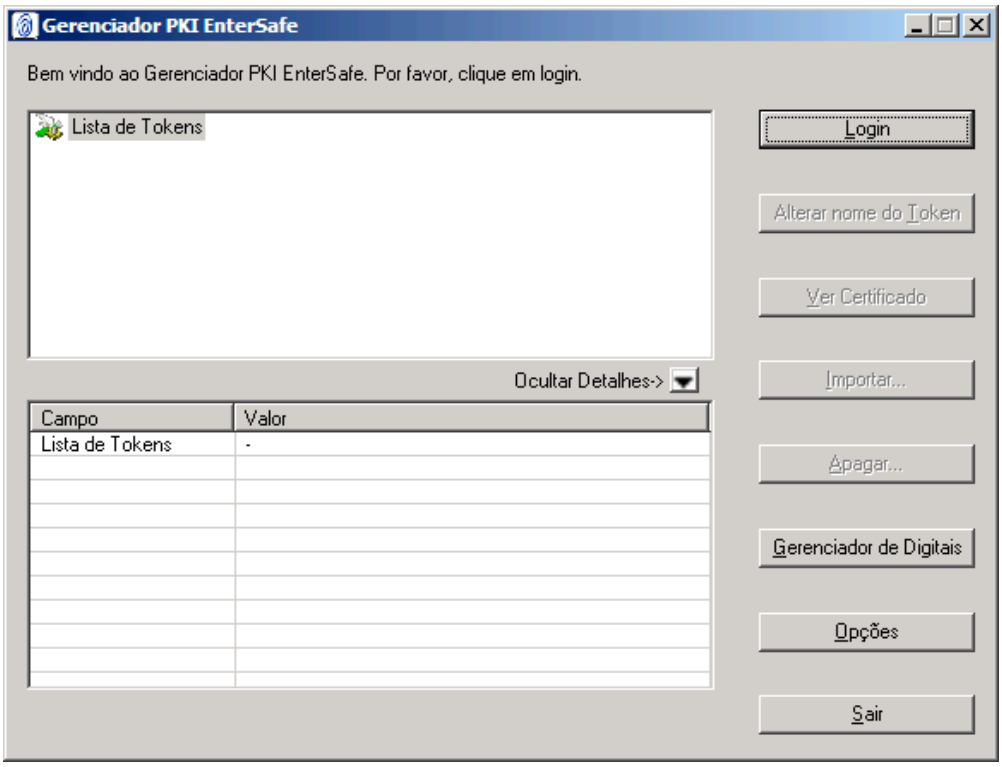


Figura 2-1-1: Interface com o token desconectado

Na parte superior da janela, todos os tokens disponíveis serão listados como "**Lista de Tokens**".

- *Interface com token conectado:* se um token chamado **BioPass Token** estiver conectado à porta USB, o Gerenciador PKI EnterSafe irá automaticamente reconhecê-lo e mostrará suas informações gerais, como na Figura 2-1-2.

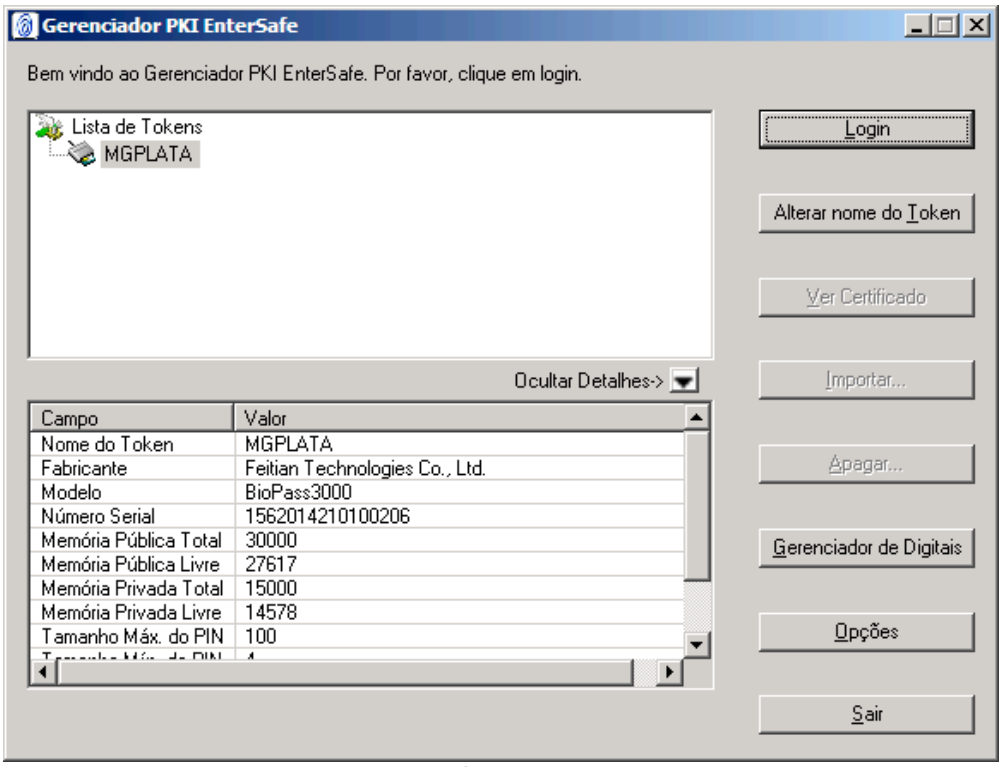


Figura 2-1-2: Interface com o token conectado

O Gerenciador PKI Entersafe oferece as seguintes opções:

Login: autenticação no Token via PIN ou via impressão digital

Alterar nome do Token: alterar o label do Token.

Ver Certificado: exibir as informações sobre o(s) certificado(s) armazenado(s) no Token

Importar: permite a importação de arquivos e chaves privadas para o Token através de um arquivo

Apagar: permite a exclusão de dados armazenados no Token

Gerenciador de Digitais: permite o cadastramento, exclusão e atualização das impressões digitais cadastradas no Token.

Opções: permite a habilitação de smart card logon em estações de trabalho rodando Windows 2000 ou versões mais recentes e outras tarefas adicionais.

Sair: botão para encerrar o Gerenciador PKI EnterSafe.

- *Informações detalhadas com o token conectado:* selecione qualquer token da lista de slots.

As informações detalhadas deste serão mostradas na parte inferior da janela, como na Figura 2-1-2.

2.1.2 Operações

- *Login:* sem fazer login, o usuário só poderá ver os objetos públicos do token. Os objetos privados só poderão ser visualizados após a verificação bem sucedida da digital. Se o usuário clicar no botão **Login**, uma caixa de diálogo de login será exibida como na Figura 2-1-9.

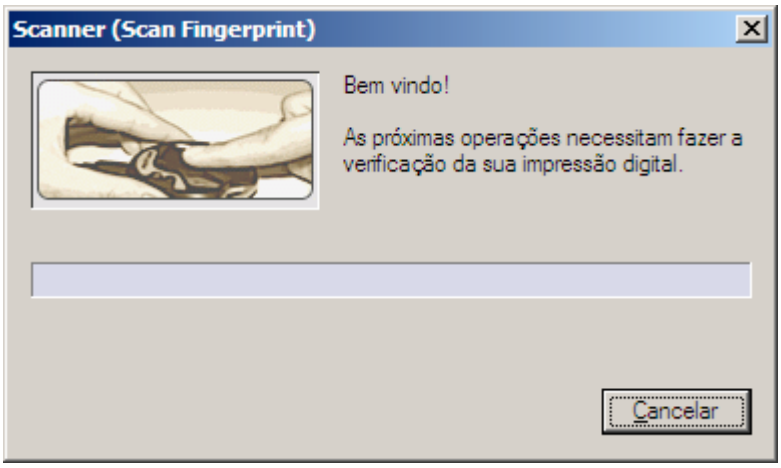

Scanner (Scan Fingerprint)
Bem vindo!
As próximas operações necessitam fazer a verificação da sua impressão digital.
Cancelar

Figura 2-1-9: Janela de login do Fingerprint Manager

Quando o usuário escolhe **Cancelar**, uma caixa de diálogo como a da Figura 2-1-10 é exibida.

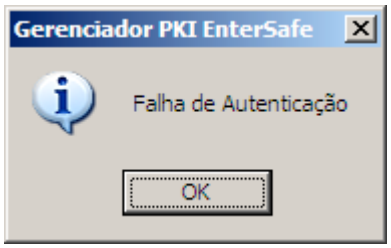


Figura 2-1-10

A caixa de diálogo irá desaparecer depois que o usuário aguardar por 10 segundos ou passar o dedo no sensor uma vez.

Após o login bem sucedido, o usuário poderá iniciar o uso do programa. Do contrário, a seguinte caixa de diálogo será mostrada. O usuário precisará verificar novamente a sua digital para fazer login.

Scanner (Scan Fingerprint)
Bem vindo!
As próximas operações necessitam fazer a verificação da sua impressão digital.
Falha ao verificar, por favor, tente outra vez
Cancelar

Figura 2-1-11

- *Alterar o nome do token:* na maioria dos casos, os tokens são distinguidos uns dos outros pelos seus números seriais. Porém, números seriais longos não são tão fáceis de ler e memorizar. Entretanto, é possível usar os nomes dos tokens para identificá-los. O nome do token também pode ser customizado.

  Se você clicar no botão **Change token name**, a seguinte caixa de diálogo é mostrada, como na Figura 2-1-12.

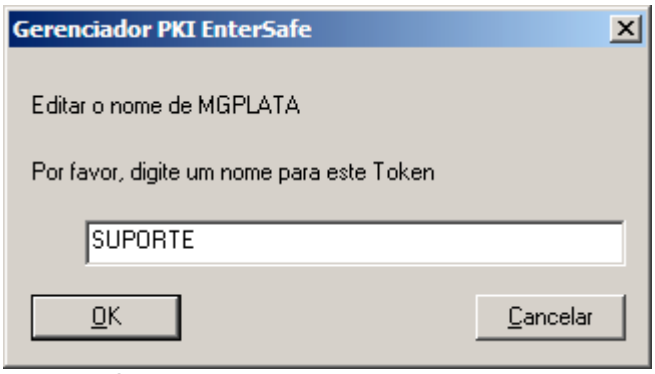


Figura 2-1-12: Caixa de diálogo de alteração do nome do token

Digite o nome desejado para o token e clique no botão **OK** para modificar. Após a troca bem sucedida do nome do token, o EnterSafe PKI Manager irá atualizar automaticamente o token com seu novo nome.

- *Gerenciamento de dados sem login de usuário:* no lado esquerdo do EnterSafe PKI Manager, cada token tem uma função de gerenciamento de dados. Se o usuário não fizer o login e clicar em **Data Management**, as informações públicas e as operações relacioandas ao token aparecerão no lado direito da janela, como mostrado na Figura 2-1-13.

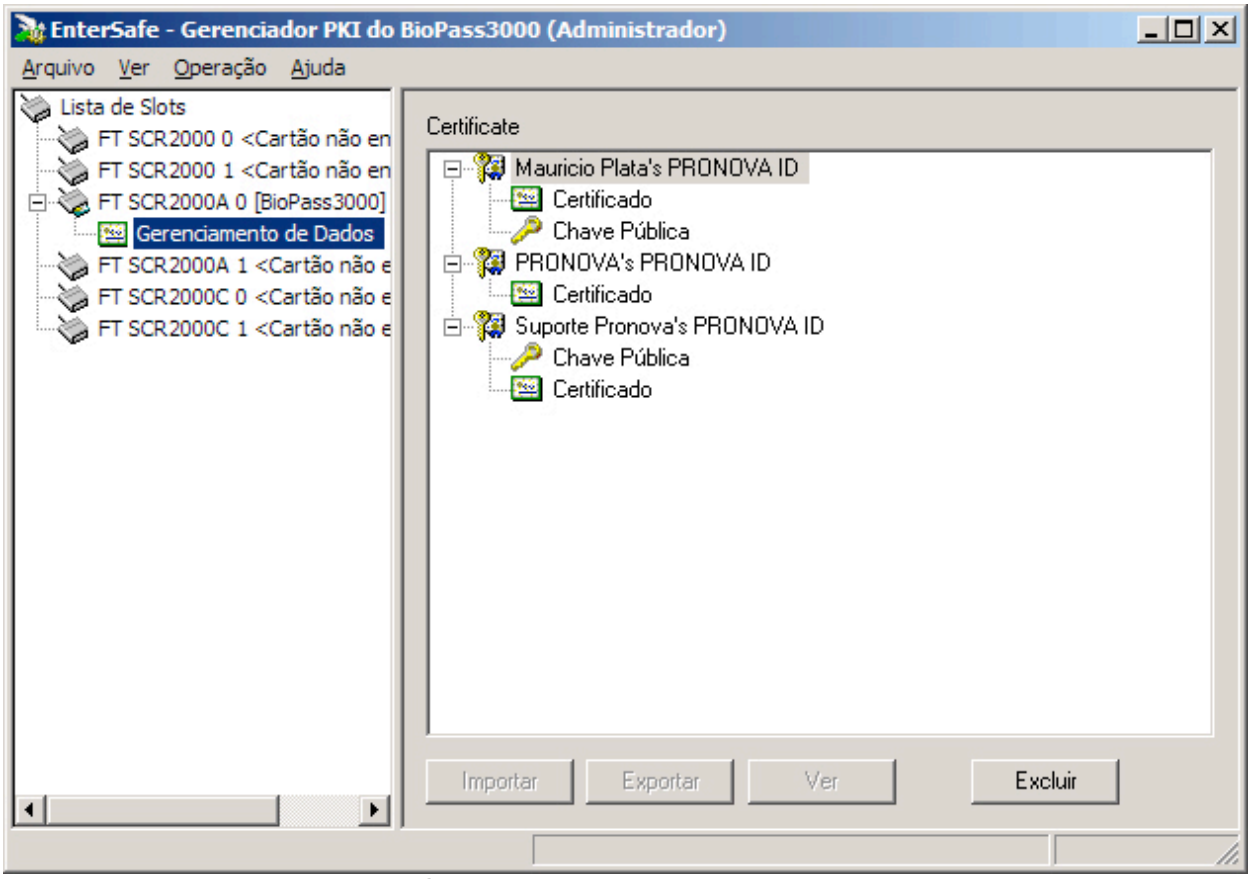


Figura 2-1-13: Gerenciamento de dados sem login de usuário

- *Gerenciamento de dados após o login do usuário:* a janela exibida após o login do usuário é como a mostrada na Figura 2-1-14.

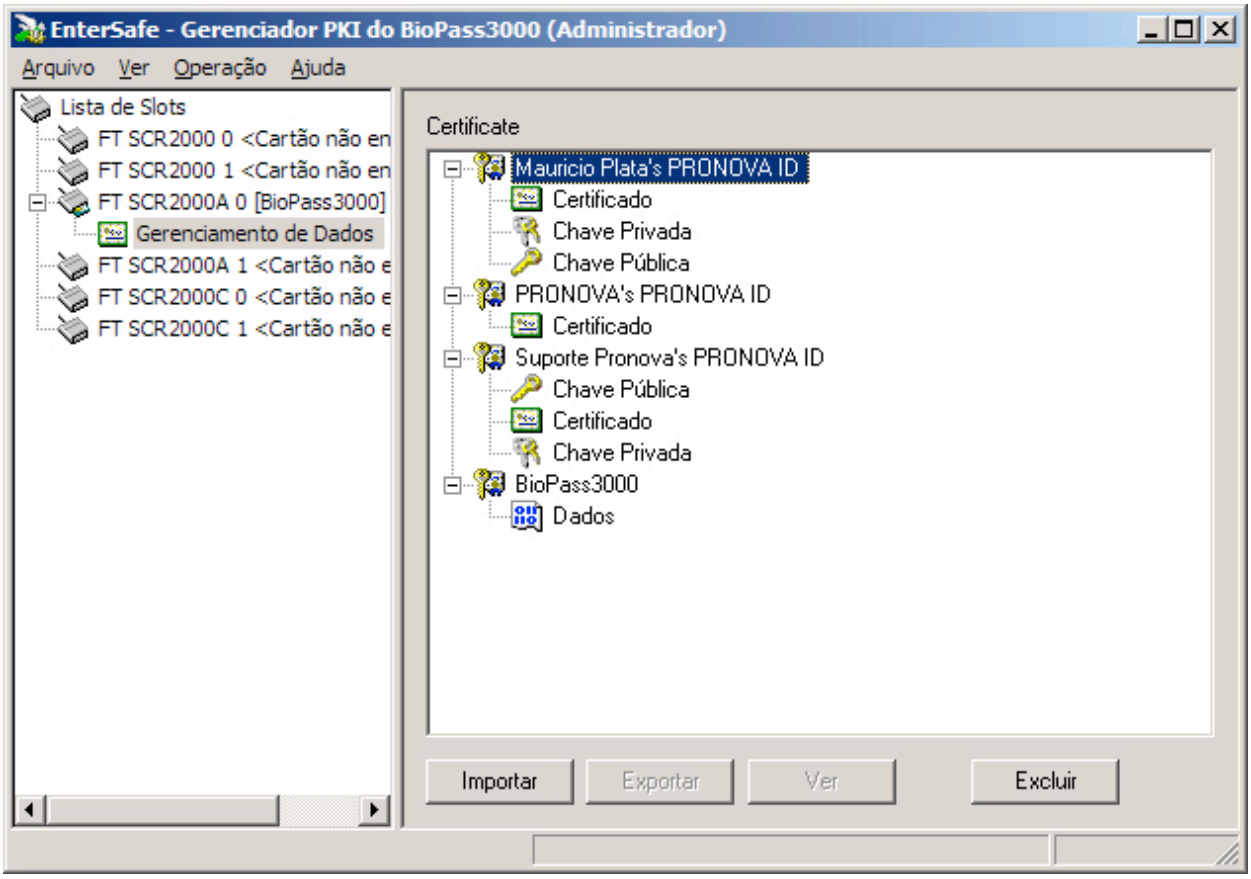


Figura 2-1-14: Janela de gerenciamento de dados após o login do usuário

Após um login bem sucedido, o usuário poderá verificar o certificado e as informações públicas e privadas contidas no token.

A função **Import** só pode ser usada após um login bem sucedido e a função **Export** só se aplica ao certificado. Já a função **View** permite que o usuário visualize qualquer informação relevante exceto o nome do token. A função **Delete** é usada para apagar todos os itens selecionados.

Nota: Esta versão do Administrador tem apenas duas opções: **Login** e **Change token name**.

Figura 2-1-15

- *Importação de certificados:* se um usuário deseja importar um certificado para o token (formatos suportados: PFX, P12, P7B, CER) basta clicar no botão **Import** para que a caixa

de diálogo **Import certificate** (Figura 2-1-16) seja exibida.

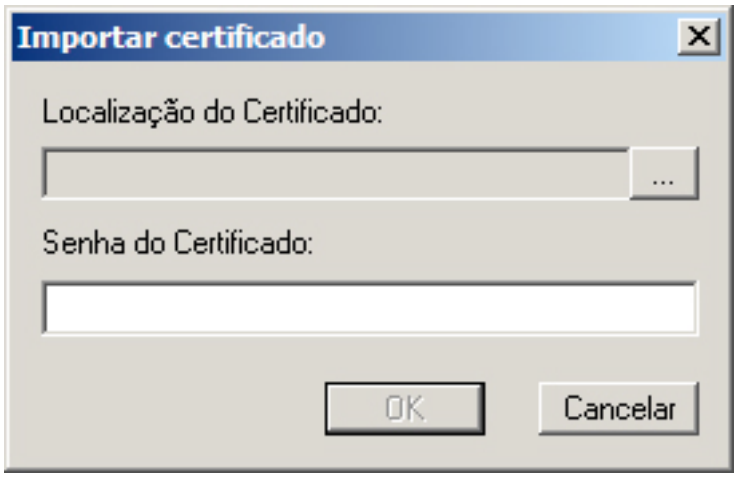


Figura 2-1-16: Caixa de diálogo1 - Import Certificate

Digite o caminho do arquivo do certificado ou clique no botão "**...**" para procurá-lo. Informe também no campo correspondente a senha do certificado e clique no botão **Ok** para realizar a importação. Veja a Figura 2-1-17.

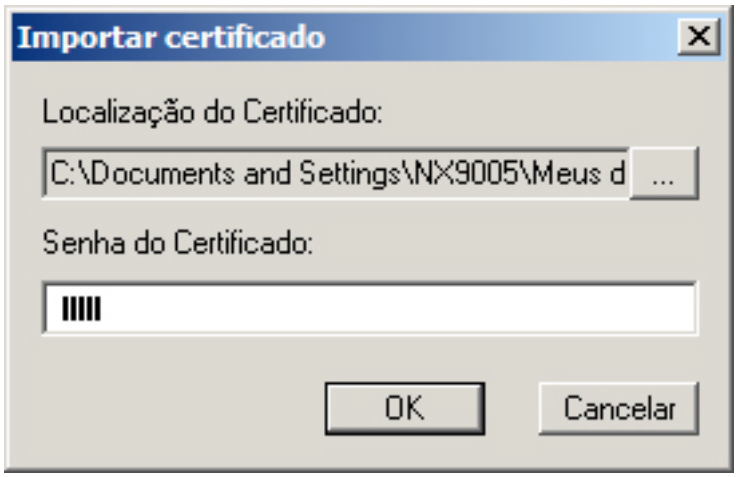


Figura 2-1-17: Caixa de diálogo 2 - Import Certificate

Notas:

1. Qualquer certificado exportado de outra aplicação PKI deve ser baseado no padrão X.509 v3 e deve incluir a sua chave privada correspondente. Ele também deve ser protegido por senha para prevenir a perda da chave privada.

2. Uma vez que o certificado com a chave privada são importados para o token, esta última não poderá ser exportada. Em outras palavras, *a chave privada nunca deixa o token*. Isso garante a integridade dos dados do certificado.

Quando o certificado P12 necessita do código de acesso ou no momento da importação de outros certificados, o sistema esconderá todas as informações relevantes. Clique no botão "**...**" para importar as informações do certificado para o token. Em seguida, o EnterSafe PKI Manager será automaticamente atualizado. Observe a Figura 2-1-18.

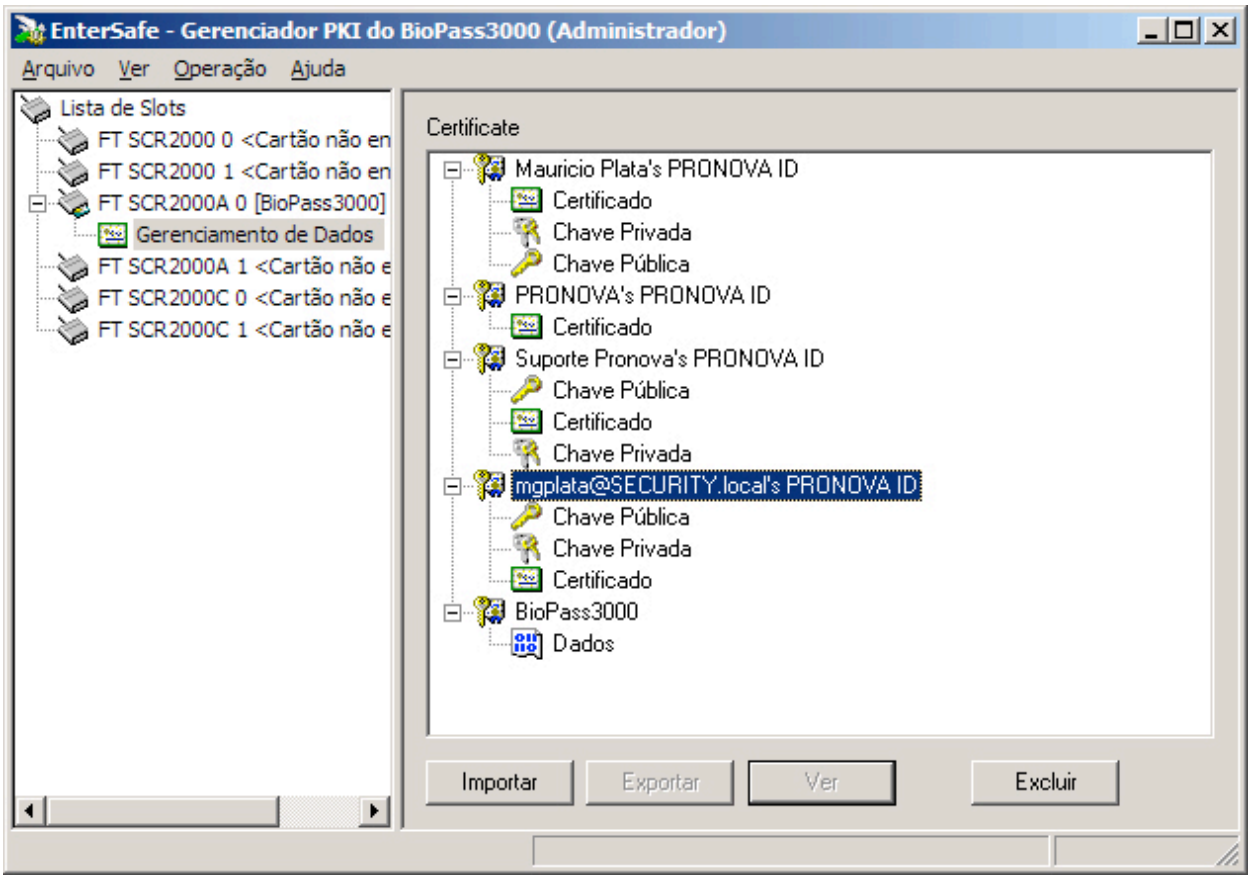


Figura 2-1-18: Janela de gerenciamento de dados após importação de um certificado

- *Exportação de certificados:* se o usuário desejar exportar um certificado basta selecioná-lo e clicar no botão **Export**. Uma caixa de diálogo como a da Figura 2-1-19 será mostrada.

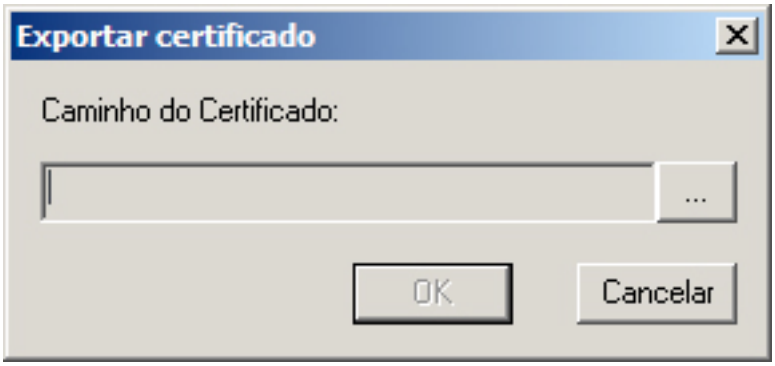


Figura 2-1-19: Caixa de diálogo Export Certificate

Clique no botão "**...**" para escolher o caminho do arquivo e em seguida clique em **Ok** para exportá-lo.

- *Display de informação de dados (Data Information Display):*

  ⇒ *Apagar certificado* - escolha na lista de certificados em **Fingerprint Manager** o certificado que deseja apagar do token e clique no botão **Delete**. O espaço antes reservado ao referido certificado será liberado.

Se o usuário quiser verificar informações do certificado como a chave pública, a chave privada ou outra informação específica basta selecionar o item referente ao certificado em questão e clicar no botão **View certificate**. Uma caixa de diálogo como a da Figura 2-1-20 será exibida.

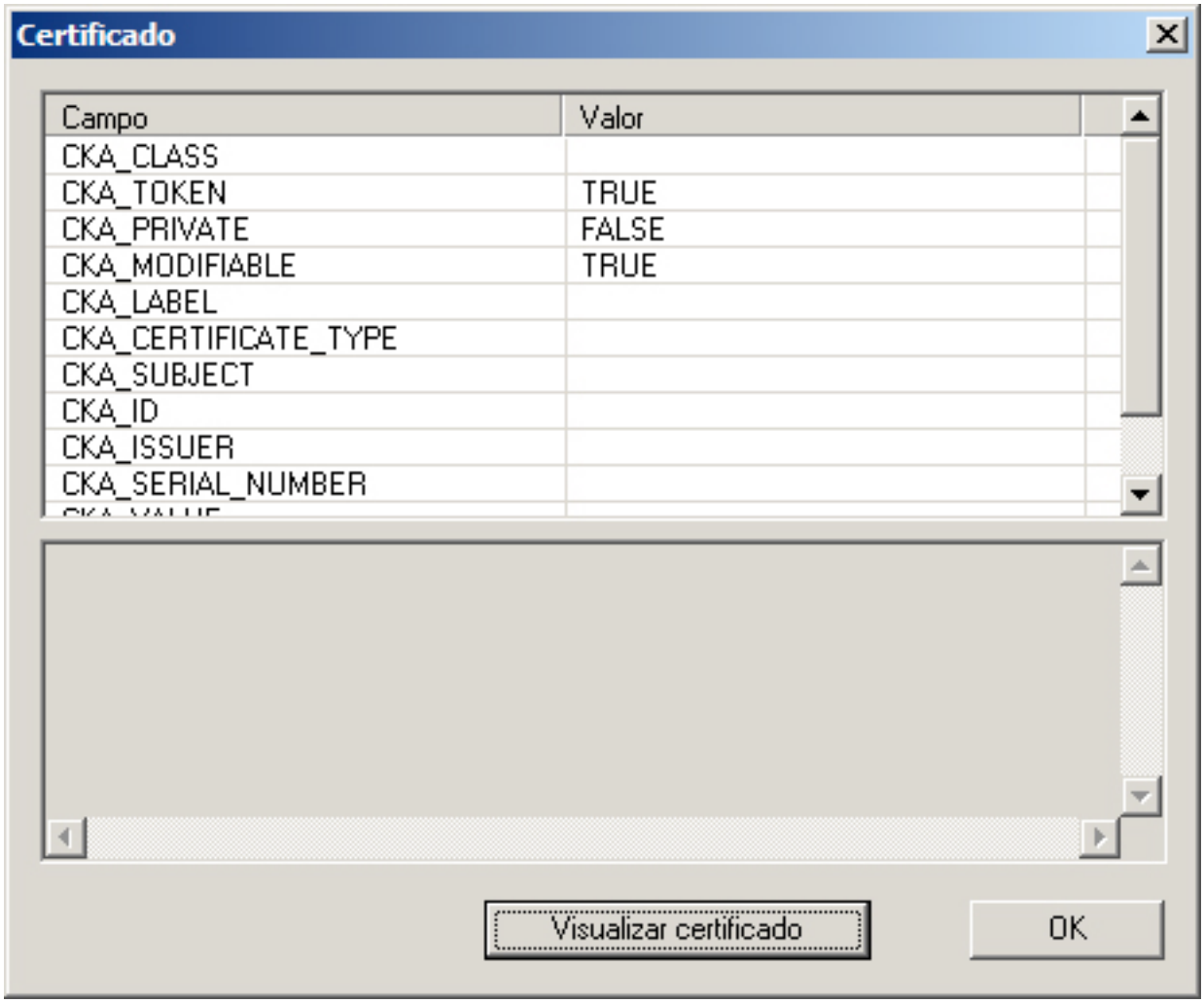


Figura 2-1-20: Janela de informações do certificado

Somente quando o conteúdo do certificado é mostrado o botão View certificate é ativado. Se você clicar nesse botão, uma janela como a da Figura 2-1-21 aparecerá.

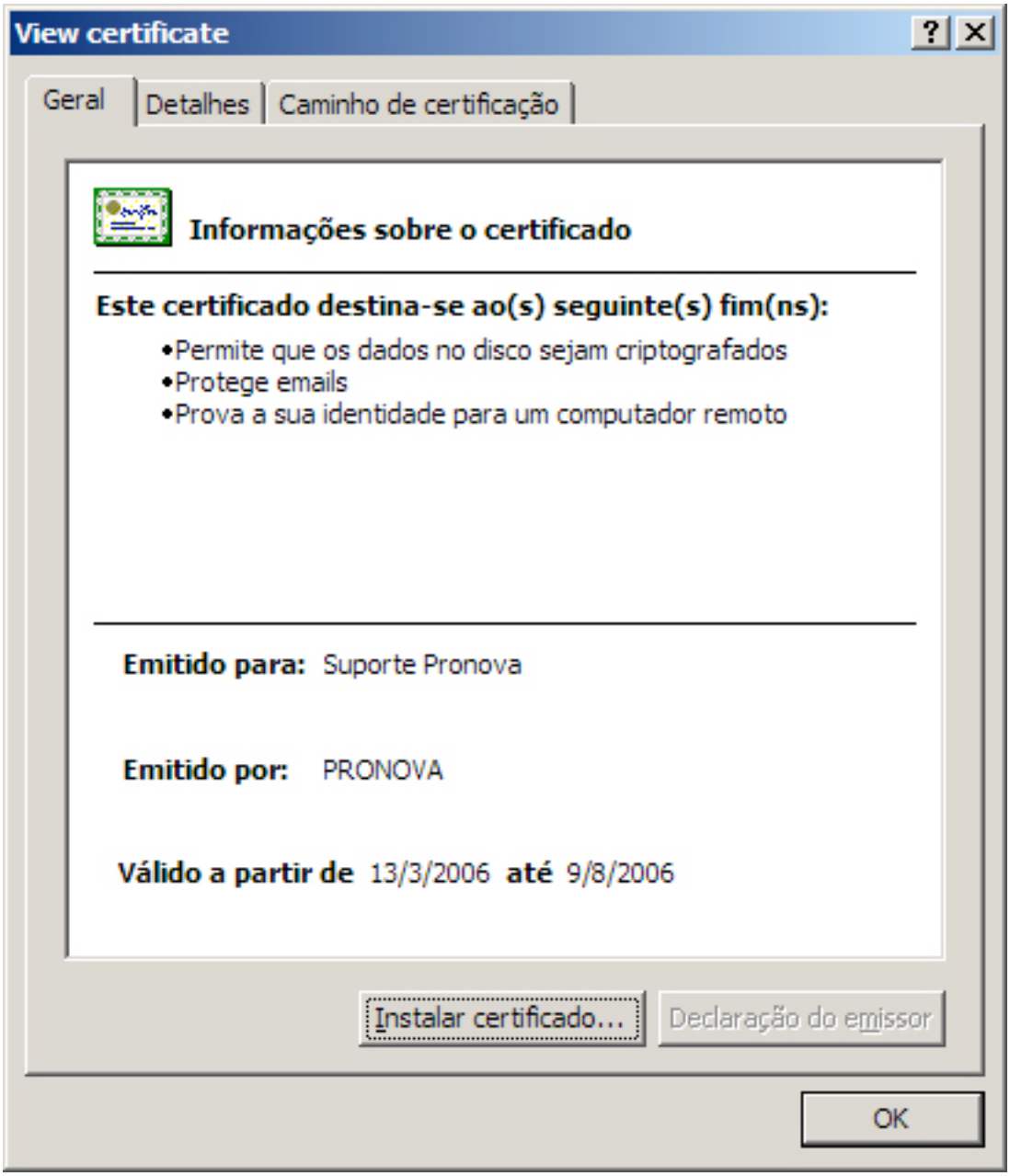


Figura 2-1-21

Ao visualizar outros dados como chave pública, chave privada etc, uma janela como a da Figura 2-1-22 será mostrada.

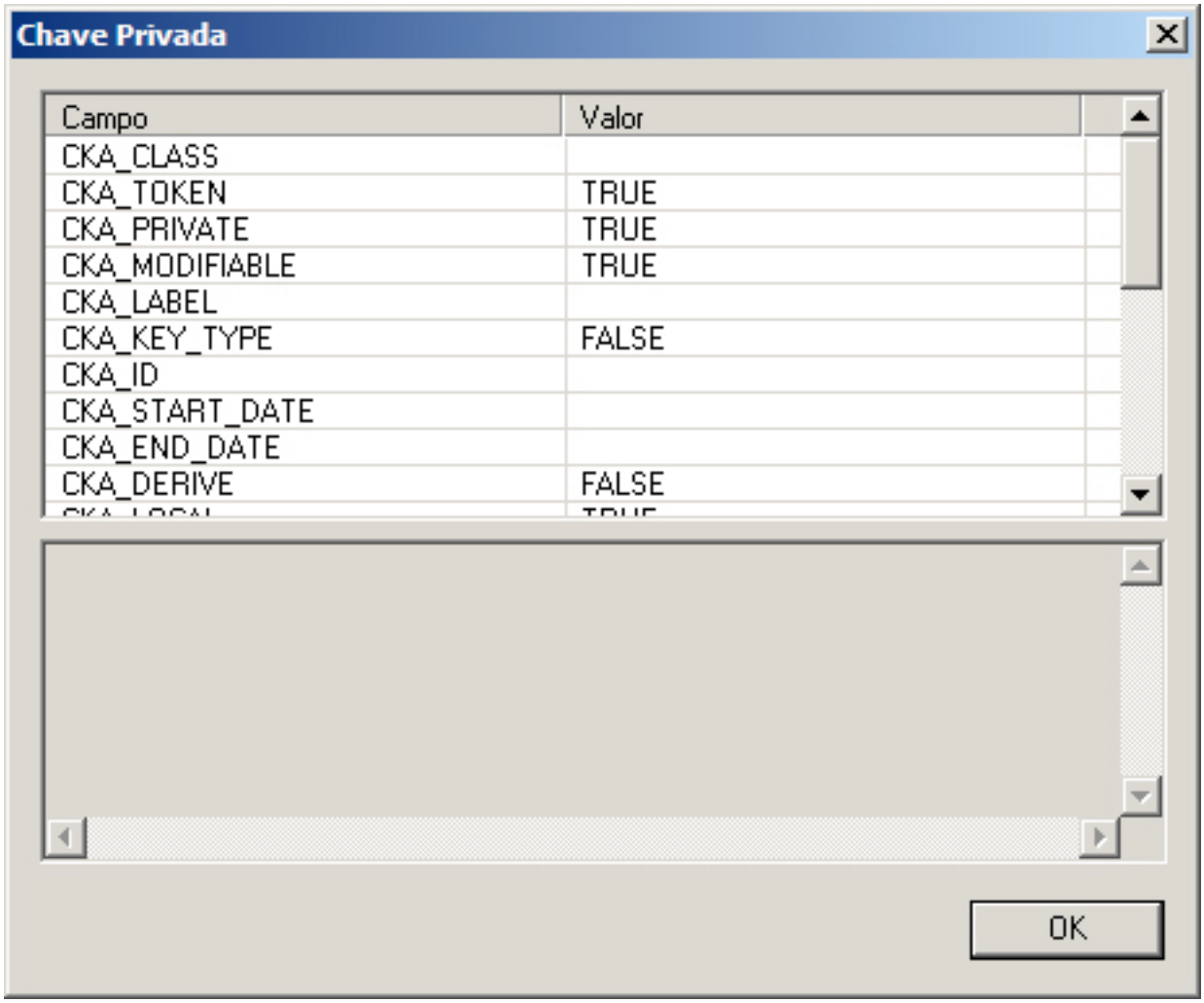


Figura 2-1-22: Janela – chave privada

⇒ *Apagar outros dados* - se o usuário quiser apagar uma informação do token ele deve fazer login e selecionar o item desejado. Em seguida, basta clicar no botão **Delete**. A caixa de mensagem mostrada na Figura 2-1-23 será exibida.

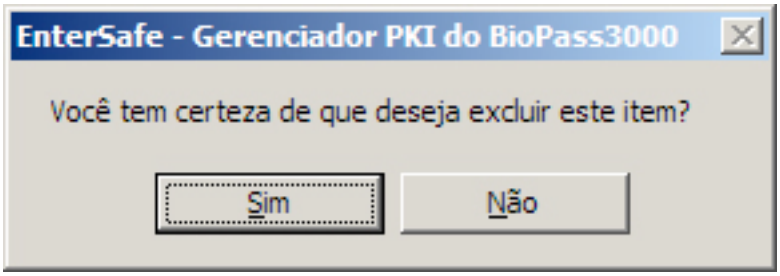


Figura 2-1-23

Clique em **Yes** para confirmar a operação. A caixa de mensagem mostrada na Figura 2-1-24 será mostrada.

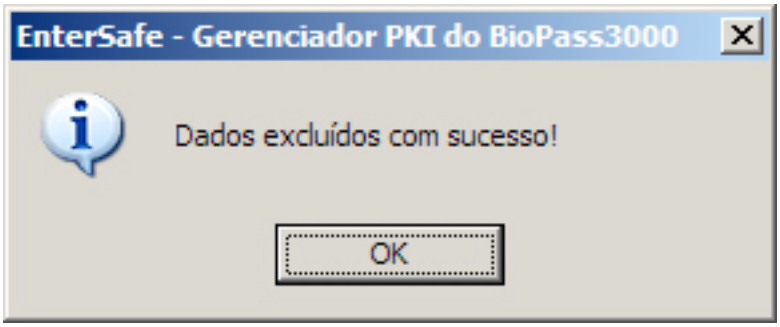


Figura 2-1-24

2.2 Fingerprint Manager

Para iniciar o aplicativo vá até **Iniciar | Programas | Feitian BioPass3000** e clique em **Fingerprint Manager**.

2.2.1 Interface

A janela principal do Fingerprint Manager contém quatro botões (veja a Figura 2-2-1) que permitem a manipulação do BioPass3000. Através deles é possível realizar as seguintes operações:

- *Verify*: verificar phrasepass (antes de cadastrar a primeira digital no token) ou verificar digital (caso esta já tenha sido previamente cadastrada);
- *Enroll*: cadastrar digital;
- *Update*: atualizar digital;
- *Delete*: apagar digital.

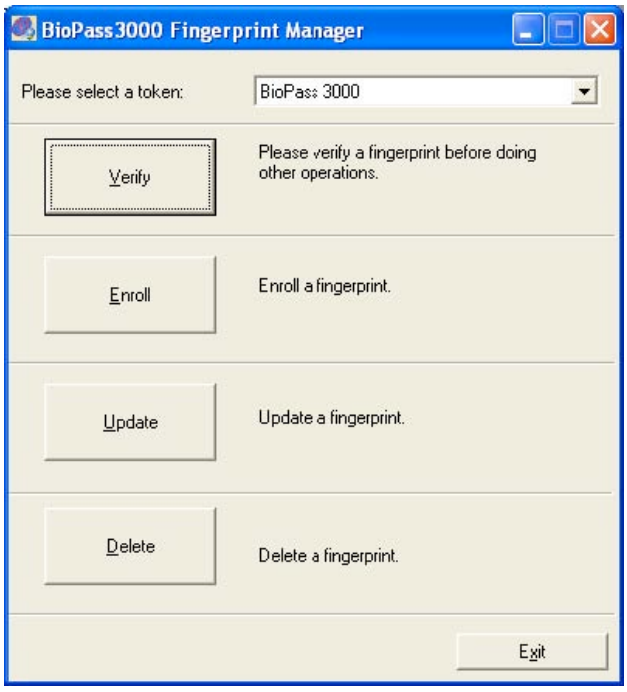


Figura 2-2-1: Janela principal do Fingerprint Manager quando um token está conectado

2.2.2 Operações

- *Verify – verificando a phrasepass:*

O primeiro passo após instalar o BioPass3000 é verificar a phrasepass e em seguida cadastrar as digitais.

Clique em Fingerprint Manager para abrir a interface deste aplicativo como mostra a Figura 2-2-1.

Conecte o BioPass3000 e selecione-o na lista de tokens onde você deseja cadastrar as suas digitais (veja a Figura 2-2-2).

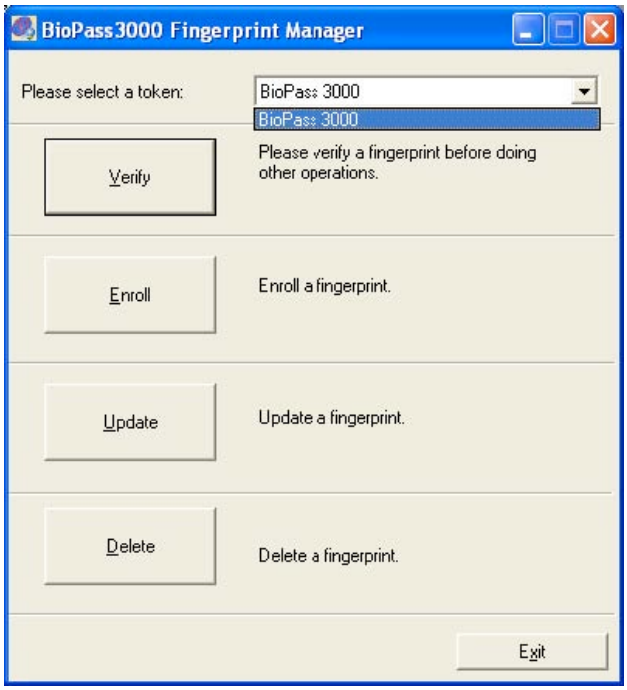


Figura 2-2-2: Fingerprint Manager – selecionando um token

Agora, você poderá verificar a phrasepass e cadastrar suas digitais. Para isso, clique em **Enroll** (como na Figura 2-2-2). Em seguida, a caixa de diálogo **Verify Phrasepass** será exibida (Figura 2-2-3).

Figura 2-2-3: Fingerprint Manager – verificando a phrasepass

No campo correspondente, digite a phrasepass **1234**.

Clique no botão **OK** para verificar a phrasepass. Se a verificação for bem sucedida, uma caixa de diálogo **Enroll**, como a da Figura 2-2-5, será exibida. Neste caso, o usuário poderá começar a cadastrar as suas digitais. Caso contrário, se a verificação falhar, uma caixa de mensagem como a da Figura 2-2-4 será exibida.

Figura 2-2-4: Fingerprint Manager – falha na verificação da phrasepass

Nota: A phrasepass é uma senha autorizada, fornecida pelo fabricante e só é válida para a primeira utilização do aplicativo, antes do cadastramento das digitais. Uma vez que uma digital for cadastrada, a phrasepass se torna inválida e não poderá ser utilizada.

- *Enroll - cadastrando uma digital:*

Após a verificação bem sucedida da phrasepass, clique no botão **Enroll**. Uma caixa de diálogo como a da Figura 2-2-5 será exibida.

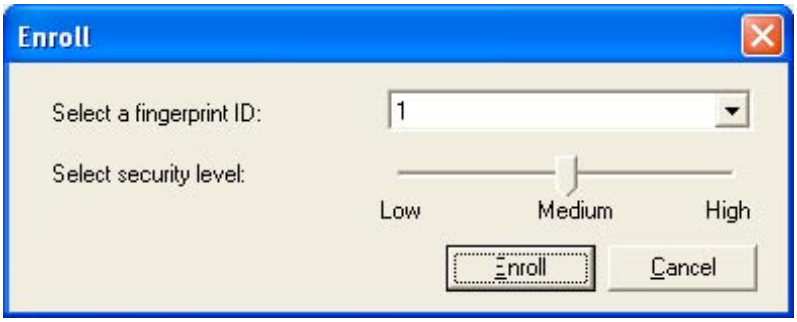


Figura 2-2-5: Fingerprint Manager – cadastrando uma digital

Escolha na lista **Select a fingerprint ID** o número atribuído à digital a ser cadastrada. Em **Select security level**, selecione o nível de segurança desejado.

Nota: Há três opções de níveis de segurança: baixo, médio e alto. Elas indicam a precisão de comparação das digitais no momento da autenticação.

Clique em Enroll para iniciar o processo de cadastramento de digitais. O usuário deverá passar o dedo no sensor três vezes para concluir o processo.

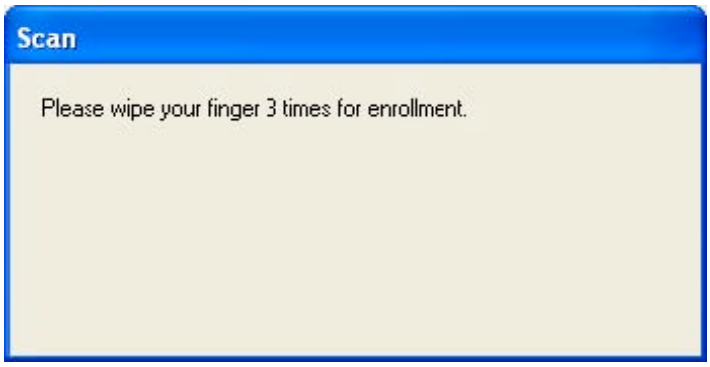


Figura 2-2-6: Fingerprint Manager – janela de cadastramento da digital

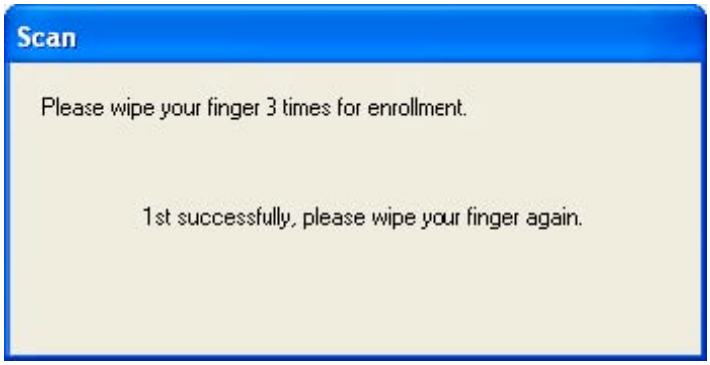


Figura 2-2-7: Fingerprint Manager - primeira imagem da 1ª digital capturada com sucesso

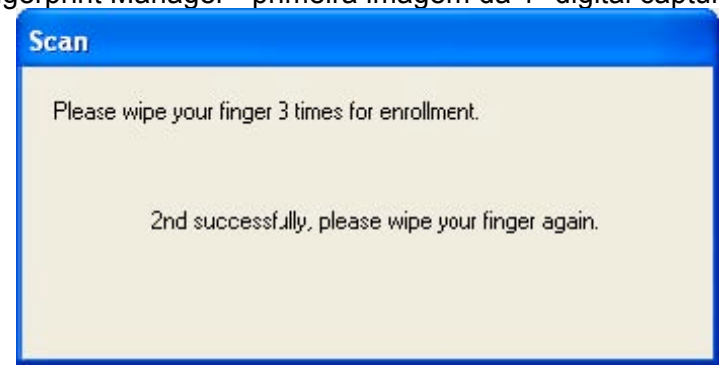


Figura 2-2-8: Fingerprint Manager – segunda imagem da 1ª digital capturada com sucesso

Figura 2-2-9: Fingerprint Manager – terceira imagem da 1ª digital capturada com sucesso

Figura 2-2-10: Fingerprint Manager – cadastramento bem sucedido de digital

Nota: Se o cadastramento de uma digital falhar, uma das caixas de mensagem mostradas na Figura 2-2-11 será exibida. O usuário poderá escolher **Yes** para tentar novamente ou **No** para cancelar.

Figura 2-2-11: Fingerprint Manager – mensagens de aviso

Nota: Recomenda-se cadastrar as digitais de mais de um dedo no token para o caso de uma das digitais sofrer algum dano acidentalmente.

- *Verify - verificando as digitais:*

Clique no botão **Verify** na caixa de diálogo como a mostrada na Figura 2-2-12.

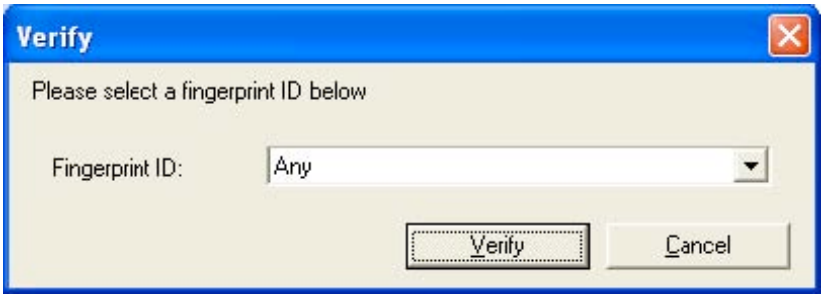


Figura 2-2-12: Fingerprint Manager – caixa de diálogo Verify

Escolha na lista **Fingerprint ID** o número de identificação da digital que deseja verificar. Se a opção **Any** for selecionada, qualquer digital cadastrada poderá ser usada para verificação. Em outras palavras, a digital apresentada pelo usuário para verificação será comparada a todas as digitais armazenadas no token. Se a comparação com qualquer uma delas for bem sucedida, então a verificação terá sido concluída também com sucesso.

Clique no botão **Verify** para que a caixa de diálogo **Scan** seja exibida, como mostrado na Figura 2-2-13.

Figura 2-2-13: Fingerprint Manager – caixa de diálogo Scan

Se a verificação for bem sucedida, uma caixa de mensagem como a da Figura 2-2-14 será exibida.

Figura 2-2-14: Fingerprint Manager – verificação bem sucedida

Em caso de falha, uma caixa com uma mensagem de erro será exibida, como mostra a Figura 2-2-15.

Figura 2-2-15: Fingerprint Manager – mensagem de erro

O usuário deverá então clicar no botão **Yes** para tentar novamente ou em **No** para cancelar a operação.

- *Update - atualizando uma digital:*

Após a verificação bem sucedida de uma digital, clique em **Update** para atualizar a digital já existente. Veja a Figura 2-2-16.

Figura 2-2-16: Fingerprint Manager – caixa de diálogo Update

Escolha na lista **Fingerprint ID** o número de identificação da digital que deseja atualizar. Uma vez que este número for selecionado, clique no botão **Update** para iniciar o processo. A caixa de diálogo **Scan** será exibida em seguida, como na Figura 2-2-17.

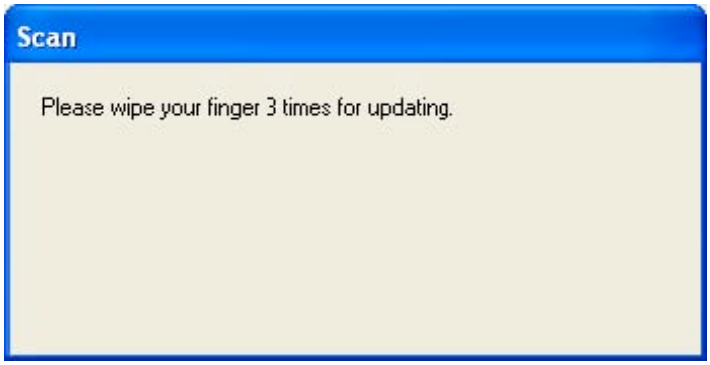


Figura 2-2-17: Fingerprint Manager – caixa de diálogo Scan

Passe o **mesmo** dedo três vezes para realizar um novo cadastramento.

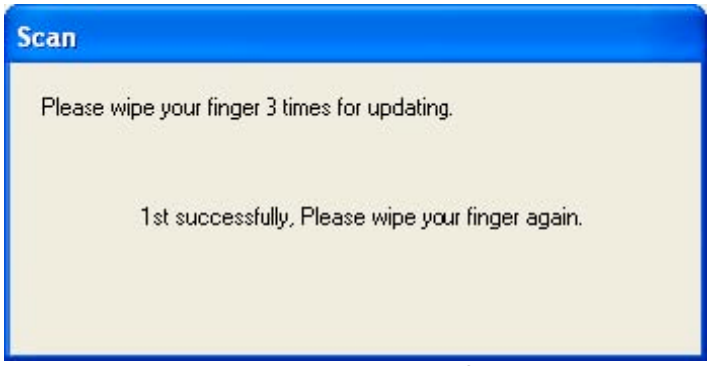


Figura 2-2-18: Fingerprint Manager – 1ª leitura bem sucedida

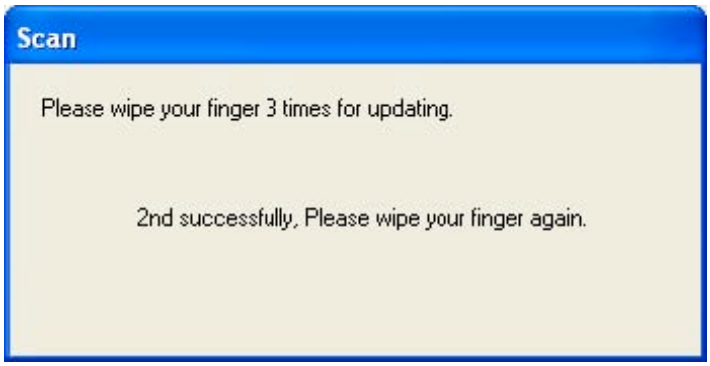


Figura 2-2-19: Fingerprint Manager – 2ª leitura bem sucedida

Figura 2-2-20: Fingerprint Manager – 3ª leitura bem sucedida

Figura 2-2-21: Fingerprint Manager – atualização realizada com sucesso

- *Delete - apagando uma digital:*

Clique no botão **Delete** para apagar uma digital previamente cadastrada. Uma caixa de diálogo será mostrada (Figura 2-2-22).

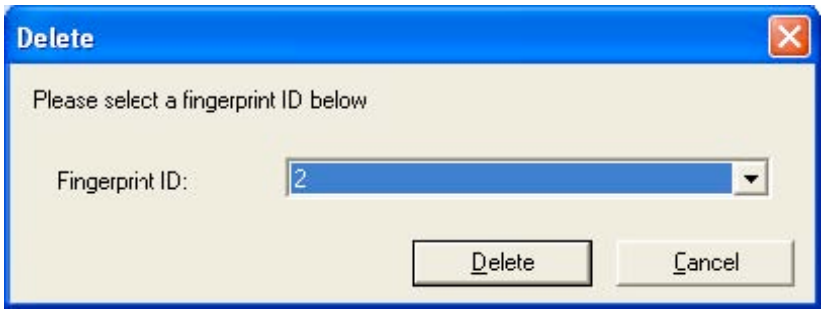


Figura 2-2-22: Fingerprint Manager – caixa de diálogo Delete

Selecione na lista **Fingerprint ID** o número de identificação da digital que deseja apagar. Em seguida, clique no botão **Delete**. Uma nova caixa de diálogo será exibida (Figura 2-2-23).

Figura 2-2-23: Fingerprint Manager – confirmação

Clique em **Yes** para apagar o item desejado (Figura 2-2-24).

Figura 2-2-24: Fingerprint Manager: operação *Delete* bem sucedida

Nota: O token não pode ser totalmente apagado se tiver alguma digital. Em outras palavras, o usuário **não pode** apagar a última digital cadastrada no token. Se um usuário tentar fazê-lo, uma caixa de mensagem será exibida, como mostra a Figura 2-2-25.

Figura 2-2-25: Fingerprint Manager – caixa de mensagem

2.3 Fingerprint Tour

O Fingerprint Tour é uma ferramenta que auxilia o usuário a cadastrar digitais corretamente.

Para iniciá-la, vá até **Iniciar | Programas | Feitian | BioPass3000** e clique em **Fingerprint Tour**.

2.3.1 Interface

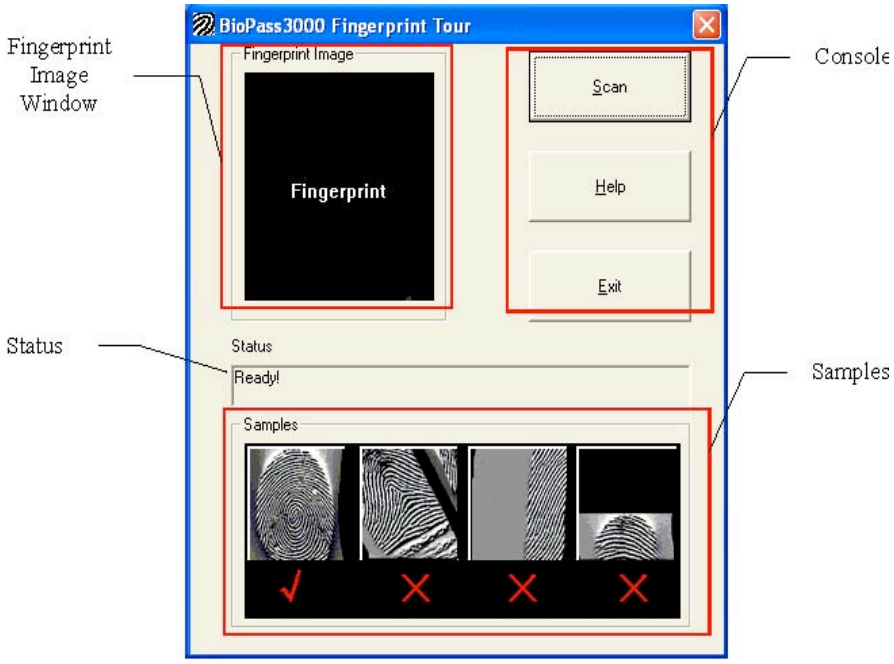


Figura 2-3-1: Fingerprint Tour – interface principal

Função		Descrição
Janela Fingerprint Image		Mostra a imagem da digital capturada
Botões	**Scan**	Clique para capturar a digital de um dedo
	Help	Clique para ler o documento de ajuda
	Exit	Clique para sair do aplicativo
Campo Status		Indica o estado atual do token
Amostras		Lista algumas amostras de digitais para comparação

2.3.2 Introdução à captura de digitais

- *Digitais qualificadas - u*ma imagem qualificada de uma digital tem as seguintes características:

  ⇒ O centro da sua digital é também o centro da imagem capturada;

  ⇒ A digital está completamente no meio da imagem sem qualquer deslocamento;

  ⇒ A imagem é clara e limpa, sem qualquer mancha;

  ⇒ A linha da digital está completa;

  ⇒ A área da imagem é quase totalmente preenchida pela digital;

  ⇒ O contraste entre as cores preta e branca é balanceado.

Exemplos de digitais qualificadas:

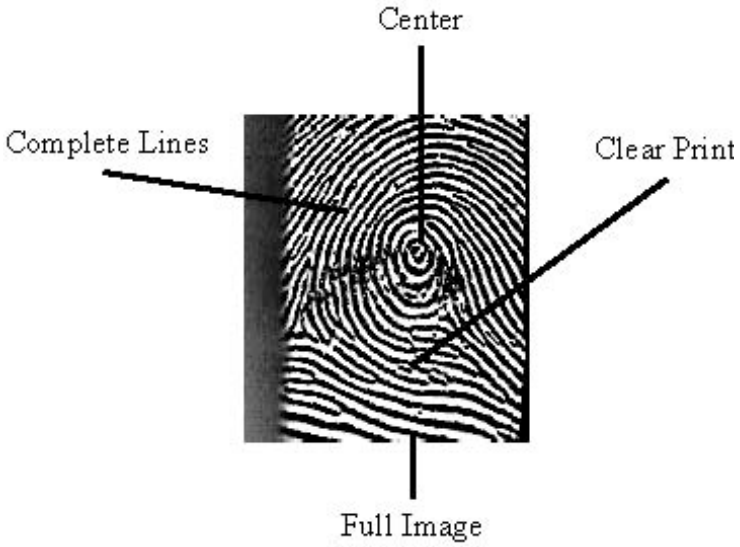


Figura 2-3-2: Uma digital qualificada

Outros:

Figura 2-3-3

Figura 2-3-4

- *Digitais não qualificadas* - abaixo são listados alguns dos motivos que podem tornar uma digital não qualificada para cadastramento no BioPass3000.

  ⇒ *Dedo molhado ou úmido* – dá origem a uma imagem escura, com contraste insuficiente para reconhecimento (Figura 2-3-5).

Figura 2-3-5

⇒ *Danos na pele do dedo* – dá origem a uma imagem imprecisa (Figura 2-3-6).

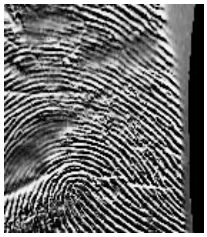


Figura 2-3-6

⇒ *Cicatrizes no dedo* (Figura 2-3-7).

Figura 2-3-7

⇒ *Atrito entre o dedo e o sensor* – dá origem a uma imagem imprecisa (Figura 2-3-8).

Figura 2-3-8

Métodos incorretos de cadastramento podem causar falhas na verificação da digital. Abaixo listamos algumas imagens não qualificadas de digitais que podem ser obtidas. Com esses exemplos o usuário será capaz de evitar determinadas maneiras de passar o dedo no sensor para não gerar uma digital não qualificada e, conseqüentemente, utilizar corretamente o BioPass3000 de modo a obter sempre digitais qualificadas.

⇒ O usuário não passa toda a superfície do dedo no sensor (Figura 2-3-9).

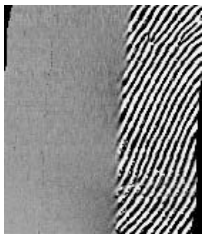


Figura 2-3-9

⇒ O usuário não passa o dedo no sensor na direção vertical (Figura 2-3-10).

Figura 2-3-10

⇒ O usuário passa o dedo muito rápido pelo sensor (Figura 2-3-11).

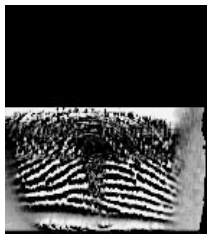


Figura 2-3-11

⇒ O usuário não passa todo o dedo no sensor – digital parcial (Figura 2-3-12).

Figura 2-3-12

⇒ Digital danificada (Figura 2-3-13).

Figura 2-3-13

CAPÍTULO 3 – Sobre o BioPass3000

3.1 Como conectar o BioPass3000

Conecte o seu BioPass3000 no computador através do cabo USB que acompanha o token, como mostra a Figura 3-1-1 abaixo.

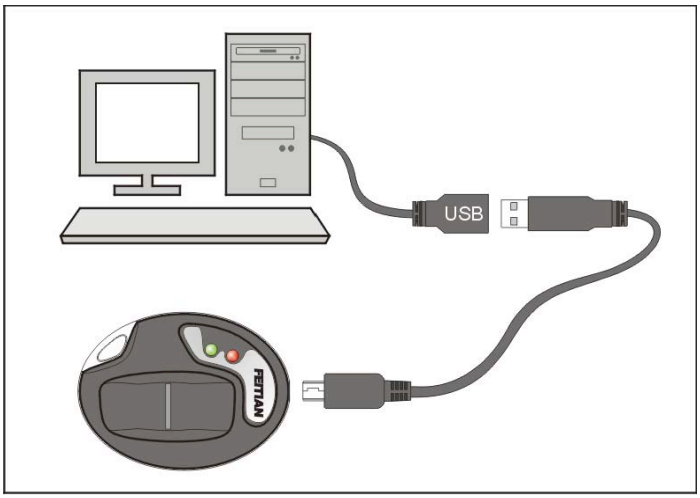


Figura 3-1-1: Conectando o BioPass3000 ao computador

Nota: Insira a mini porta USB no token e a porta USB padrão no computador (Figura 3-1-1).

3.2 Como manusear o BioPass3000

Figura 3-2-1

3.3 Como passar o dedo no sensor

Passe o dedo de um lado a outro do sensor mantendo a direção vertical.

Figura 3-3-1

Figura 3-3-2

3.4 Exemplos

3.4.1 Como usar o Fingerprint Tour para coletar uma amostra

Depois de conectar o BioPass3000 abra o Fingerprint Tour e clique no botão **Scan**. A LED vermelha do token se acenderá como na Figura 3-4-1. Em seguida, passe o dedo no sensor. Quando a digital for mostrada na área **Fingerprint Image** da janela, compare a imagem obtida com os exemplos fornecidos no próprio aplicativo para concluir se esta é uma digital qualificada para cadastramento.

Figura 3-4-1

Nota: Após clicar no botão **Scan** e antes de passar o dedo no sensor **NÃO** clique em **Exit**. Se o usuário quiser sair do aplicativo nesse momento ele deve aguardar 10 segundos ou então passar o dedo no sensor (Figura 3-4-2) e somente em seguida clicar no botão **Exit**.

Figura 3-4-2

Passe o dedo pelo sensor fazendo uma leve pressão e na velocidade adequada – nem muito rápido, nem muito devagar. Esse movimento requer uma certa prática para que se obtenha uma digital qualificada. Utilize o Fingerprint Tour para praticar quantas vezes for necessário.

Figura 3-4-3

Figura 3-4-4

3.4.2 Como usar o Fingerprint Manager para cadastrar uma digital

Quando a janela da Figura 2-2-6 aparecer, passe o dedo como mostrado na Figura 3-4-3. A LED vermelha do BioPass3000 se apagará quando o cadastramento for concluído.

3.4.3 Como usar o EnterSafe PKI Manager para login

Quando a janela da Figura 2-1-9 aparecer, passe o dedo como mostrado na Figura 3-4-3. A LED vermelha do BioPass3000 se apagará quando o cadastramento for concluído.

APÊNDICE 1

Especificações Técnicas

Hardware	Voltagem de Operação	5V via porta USB	
	Consumo de Energia	80 - 150mA	
	Temperatura de Operação	5 - 40°C	
	Temperatura de Armazenamento	0 - 50°C	
	Taxa de Umidade	20 ~ 80%	
	Chassi	Plástico resistente moldado	
	Conector	Mini porta USB	
	Microprocessador	32 Bits	
	Espaço de Armazenamento	64KB	
	Reescritas em células de memória Flash	Aproximadamente 100.000 vezes	
	Retenção de dados na memória	Aproximadamente 100 anos	
	Vida útil do sensor	Aproximadamente 100.000 vezes	
	ESD	On pins. HBM (Human Body Model) CMOS I/O	≤ 2KV
		On die surface (Zapgun Air discharge)	± 16KV

Software	Acquisition Timing	< 1S
	Tempo de Identificação	Inferior a 1 segundo
	Modo de validação	1:1; 1:N
	Taxa de falso positivo	0.1% ~ 0.01%
	Taxa de falso negativo	0.01% ~ 0.001%
	Número máximo de digitais armazenadas	Aproximadamente 8
	Níveis de comparação	3
	Número de tentativas de identificação de uma digital	ilimitado
	Indicadores de estado	2 LEDs
	API & padrões suportados	PKCS # 11 v2.11, MS CAPI, PC/SC, X.509 v3 Store Certificate, SSL v3, IPSec, ISO 7816 Compliant
	Algoritmos de criptografia no chip	RSA, DES, 3DES, MD5, SHA-1
	Nível de segurança do chip	Dados criptografados
	Sistemas Operacionais suportados	Windows 98SE/Me/2000/XP/2003

APÊNDICE 2

Glossário de Termos

Palavras-chave e termos	Descrição
BioPass3000	Token biométrico portátil baseado em um cartão inteligente desenvolvido pela Feitian. Combina um módulo sensor de digitais e um módulo de verificação de digitais. Com as digitais armazenadas em seu chip, o BioPass3000 usa a verificação única das mesmas em lugar da verificação tradicional baseada em senha. Possui todas as vantagens de um cartão inteligentes (smart card).
Token	Nome genérico para dispositivos criptográficos portáteis. Pode ser um cartão inteligente ou qualquer dispositivo de hardware com capacidade para armazenar senhas e/ou certificados.
Token USB	Dispositivo criptográfico com uma porta USB. Fácil de transportar e usar. O BioPass3000 é um exemplo de token USB.
EnterSafe	Framework de middleware seguro, suporta vários tokens.
Phrasepass	Código de ativação padrão autorizado e assinado pelo fabricante.
Interface Crypto API (CAPI)	Interface de Programação de Aplicações Criptográficas da Microsoft. Contém funções que permitem que aplicações baseadas em Windows criptografem ou assinem digitalmente dados de maneira flexível, ao mesmo tempo que oferecem proteção para os dados sensíveis como as chaves privadas do usuário.
Interface PKCS#11	Os Padrões de Criptografia de Chave Pública (*Public-Key Cryptography Standards* ou PKCS) são um conjunto de padrões desenvolvidos pela RSA, em colaboração com um consórcio informal que originalmente incluía a Apple, Microsoft, DEC, Lótus, Sun e MIT. Os padrões PKCS foram citados pelo OIW (OSI Implementers' Workshop) como um método para implementar os padrões OSI. Os padrões PKCS foram desenvolvidos para dados binários e ASCII. Também são compatíveis com o padrão ITU-T X.509. O padrão PKCS#11 define uma interface de programação independente de tecnologia chamada Criptoki, para dispositivos criptográficos como cartões inteligentes (smart cards) e cartões PCMCIA.